

Norma Tecnológica SCADA (Sistemas de Control Industrial)

El contenido de este documento es propiedad de Aena, no pudiendo ser reproducido, ni comunicado total o parcialmente a otras personas distintas de las incluidas en esta lista de distribución adjunta a este documento, sin la autorización expresa de Aena.

Documentación

Copia nº 00/00

Título

Norma Tecnológica SCADA (Sistemas de Control Industrial)

Código Código	Versión 2.0	Fecha Versión 22/11/2019
Clasificación ☐ Público ☐ Interno ☒ Restringido ☐ Confidencial	Tipo de Documento ☒ Documento técnico ☐ Presentación ☐ Propuesta/Informe ☐ Otros:	Estado ☒ Borrador ☐ En revisión ☐ Actualizable ☐ Informe final
Nombre del fichero	Norma Tecnológica SCADA.docx	
Ruta del archivo	[]	
Palabras clave	[]	

Resumen del contenido

[...]

Control de la documentación

	Nombre / Puesto	Firma / Fecha
Realizado	Beatriz Caballero Bernalte Getronics	☒ Documento firmado el día 10 de enero de 2020 a las 10:26 horas Por Beatriz Caballero Bernalte Clave de verificación: 1578648400474G
	Francisco Galisteo González Getronics	☒ Documento firmado el día 10 de enero de 2020 a las 13:34 horas Por Francisco Galisteo González Clave de verificación: 1578648400474G
	Víctor Díaz. Jefe del Departamento de desarrollo de aplicaciones de Control y Mantenimiento de Infraestructuras	☒ Documento firmado el día 10 de enero de 2020 a las 14:14 horas Por Víctor Díaz Monzon Clave de verificación: 1578648400474G
	Cándido Arregui. Jefe del Departamento de Seguridad TIC / CISO	☒ Documento firmado el día 13 de enero de 2020 a las 07:44 horas Por Candido Arregui Hernandez Clave de verificación: 1578648400474G
	Ángel de Antonio García. Jefe Departamento Centro Control de Red	☒ Documento firmado el día 13 de enero de 2020 a las 08:17 horas Por Angel Luis de Antonio Garcia Clave de verificación: 1578648400474G
	José Ángel Moreno Orgaz. Jefe Departamento Sistemas de Red y Microinformatica	☒ Documento firmado el día 15 de enero de 2020 a las 13:36 horas Por Aurelio Lopez Gonzalez Clave de verificación: 1578648400474G Por delegación de Jose Angel Moreno Orgaz
Revisado	José Luis Cuenca. Jefe de la División de Desarrollo de Aplicaciones Aeroportuarias	☒ Documento firmado el día 16 de enero de 2020 a las 17:09 horas Por Jose Luis Cuenca Casas Clave de verificación: 1578648400474G
	Emilio Prado. Jefe de la División de Comunicaciones	☒ Documento firmado el día 17 de enero de 2020 a las 08:10 horas Por Emilio Prado Diaz Clave de verificación: 1578648400474G

	Aurelio López. Jefe de la División de Sistemas	☒ Documento firmado el día 20 de enero de 2020 a las 09:47 horas Por Aurelio Lopez Gonzalez Clave de verificación: 1578648400474G
	Blas Zamorano. Jefe de la División de Instalaciones Aeroportuarias	☒ Documento firmado el día 22 de enero de 2020 a las 16:15 horas Por Blas Zamorano Gordon Clave de verificación: 1578648400474G
	Julio Antoñanzas. Gerente de Proyectos de Sistemas Eléctricos y Balizamiento	☒ Documento firmado el día 22 de enero de 2020 a las 16:37 horas Por Julio Antoñanzas Mejia Clave de verificación: 1578648400474G
	Loreto Fraile. Jefa de la División de Ingeniería	☒ Documento firmado el día 22 de enero de 2020 a las 22:25 horas Por Loreto Fraile Diez Clave de verificación: 1578648400474G
	Juan Carlos Palomero. Jefe de la División de Construcción	☒ Documento firmado el día 23 de enero de 2020 a las 07:28 horas Por Juan Carlos Palomero Arranz Clave de verificación: 1578648400474G
Aprobado	Eloy Barragán. Director de Tecnologías de la Información y Comunicaciones	☒ Documento firmado el día 23 de enero de 2020 a las 09:15 horas Por Eloy Barragan Gallego Clave de verificación: 1578648400474G
	Antonio Rosselló. Director de Proyectos y Construcción	☒ Documento firmado el día 27 de enero de 2020 a las 18:34 horas Por Antonio Rossello Caldentey Clave de verificación: 1578648400474G
Conforme	Mariano Domingo. Director de Infraestructuras y Tecnología	☒ Documento firmado el día 28 de enero de 2020 a las 12:41 horas Por Mariano Domingo Calvo Clave de verificación: 1578648400474G

Copia	Nombre	Puesto	Organización
1	Responsables Informática	Aeropuertos	Aena

Control de la distribución

Versión	Fecha	Páginas afectadas	Notas y razones del cambio
1.0	13/08/2019	TODAS	[...]
2.0	22/11/2019	TODAS	Revisión arquitecturas

Hoja de registro de cambios

Contenido

1	Introducción	7
1.1	Objeto y alcance	7
1.2	Glosario de Términos	8
1.3	Revisión de la Norma Tecnológica SCADA	9
1.4	Excepciones a la Norma Tecnológica SCADA	9
1.5	Cláusula de Cumplimiento de la Norma Tecnológica SCADA.	9
1.6	Cláusula de Auditoría.	9
2	Arquitectura del Sistema	10
2.1	Diseño arquitectura	10
2.1.1	Arquitectura para el Modelo de Desarrollo 1	11
2.1.2	Arquitectura para el Modelo de Desarrollo 2	14
2.1.3	Comunicaciones permitidas	18
2.1.4	Red de Servicios.....	19
2.2	Securización.....	20
2.2.1	Separación de Redes IT/OT	20
2.2.2	Segmentación de Redes OT	22
2.3	Requisitos de Ingeniería de Sistemas de Control.....	25
2.3.1	Arquitectura Software	25
2.3.2	Redundancia.....	26
2.3.3	Tecnologías	26
2.3.4	Gestión de alarmas y eventos	27
2.3.5	Navegación por la aplicación.....	27
2.4	Requisitos del sistema de control SCADA.....	27
2.4.1	Disponibilidad del Sistema SCADA.	27
2.4.2	Planificación de recuperación del sistema	27
2.4.3	Seguridad y acceso al sistema.....	28
2.4.4	Documentación exigida	29
3	Seguridad aplicada a los sistemas SCADA	30
3.1	Requisitos de seguridad.....	30
3.1.1	General	30
3.1.2	Cumplimiento de las leyes territoriales e internacionales	30
3.1.3	Responsabilidades y obligaciones	31
3.1.4	Interlocutor de Seguridad.	32
3.1.5	Soporte ante incidentes.	33
3.2	Estudio de seguridad	33
3.2.1	Análisis de Riesgos.	33
3.2.2	Medidas de Protección Básica.	34
4	Mantenimiento de los sistemas	49

1 Introducción

Los Sistemas de Control y SCADA de Aena son cada vez más convergentes y dependientes de las tecnologías IT clásicas. Estas tecnologías como TCP/IP, navegadores Web y las tecnologías inalámbricas, que aportan beneficios empresariales positivos, también conllevan dos problemas importantes.

Por un lado, los Sistemas de Control que tradicionalmente habían sido pensados para llevar a cabo las tareas de controlar y proteger, y que en un principio estaban aislados, se están conectando a redes abiertas (obligados por la necesidad de conectividad al ser necesario por ejemplo extraer información de la instalación), exponiéndose de esta forma a amenazas tipo malware, hackeos, etc.

Por otro lado, el software comercial y el hardware de propósito general utilizados en la implementación de Sistemas de Control y SCADA, no permiten adoptar las medidas estándar de protección de la seguridad TI.

En el caso de que estas vulnerabilidades fueran explotadas, las consecuencias podrían ser muy negativas, ya que cualquier cambio o modificación en las condiciones de funcionamiento de algunos sistemas críticos de los aeropuertos, puede conllevar la degradación de las condiciones de operación además de pérdida de integridad y confidencialidad, cuyo resultado final sea un impacto negativo en la reputación empresarial.

Con el fin de gestionar y combatir estos riesgos en los sistemas de control de Aena, así como otras deficiencias observadas a lo largo de estos años, este documento describe los procedimientos para homogeneizar las arquitecturas necesarias para el despliegue de sistemas y procesos, garantizando su funcionamiento óptimo y minimizando los riesgos que afectan a la red operacional.

Además, este documento es la base y el punto de partida de un proceso iterativo que garantiza que los cambios en las amenazas, los riesgos y las medidas para las distintas unidades operacionales se pueden incorporar en el concepto de seguridad de manera estructurada.

1.1 Objeto y alcance

El objetivo de esta norma es definir los requisitos y directrices mínimos obligatorios que rigen el desarrollo, implantación y el mantenimiento de los sistemas de control de supervisión y adquisición de datos (SCADA) de Aena. Esta norma establece los criterios de arquitectura, desarrollo y seguridad a adoptar para realizar estas tareas con garantía, seguridad y criterios de aislamiento.

La Norma Tecnológica SCADA está destinada a promover, regir y apoyar la implantación de medidas técnicas en los sistemas SCADA (las medidas organizativas, de aplicación también en esta Norma, están descritas en el documento “Norma Organizativa de Sistemas SCADA”).

La presente norma es de obligado cumplimiento para todo el personal relacionado con la gestión, operación y mantenimiento de los sistemas SCADA utilizados por la organización. Esto incluye a trabajadores internos y externos, así como trabajadores eventuales y terceras partes.

El cumplimiento de la Norma Tecnológica SCADA deberá garantizar en todo momento la seguridad de la información en relación a su

- Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada
- Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Esta Norma es de aplicación a todos los sistemas SCADA de la red de aeropuertos de Aena, sin excepción.

1.2 Glosario de Términos

ANS	Acuerdo de Nivel de Servicio.
BBDD	Bases de Datos
CIONA	Control Instalaciones y Oficina de Normalización de Aena
CPD	Centro de Procesos de Datos
DPC	Dirección de Proyectos y Construcción
DTIC	Dirección de Tecnologías de la Información y Comunicaciones
DCOM	División de Comunicaciones.
DGS	División de Gestión de Sistemas.
ET	Edificio Terminal
HMI	Human Machine Interfaces
HW	Hardware
IT	Tecnologías de la Información.
NTS	Norma Tecnológica SCADA
OEM	Original Equipment Manufacturer
OSTIC	Oficina Seguridad. de Tecnologías de la Información y Comunicaciones.
OT	Tecnologías de la Operación.
PLC	Programmable Logic Controller
RD	Real Decreto
RCC	Regulador de Corriente Constante
SCADA	Supervisory, Control and Data Acquisition
SMPB	Sistema de Mando y Presentación de Balizamiento.
SIEB	Sistema de Inspección de Equipaje en Bodega
SATE	Sistema Automático de Tratamiento de Equipajes
SIGMA	Sistema Integrado de Gestión y Monitorización de Asistencia
SITIA	Sistema Integrado de Torres de Iluminación Aeroportuaria
SCI	Sistema de Control de Instalaciones
UPS	Uninterruptible Power Supply
VLAN	Red de Area Local Virtual
WAS	Wonderware Application Server

1.3 Revisión de la Norma Tecnológica SCADA

La Norma Tecnológica SCADA será objeto de revisión *bienal* siempre y cuando no se presenten cambios significativos tales como nuevas amenazas o riesgos, nueva legislación, etc., que obliguen a su revisión inmediata, o si de las conclusiones del proceso de análisis de los distintos sistemas SCADA existentes en Aena se imponga la necesidad de proceder a su modificación y mejora.

La revisión de la Norma Tecnológica SCADA será analizada y propuesta por el Comité de Análisis y Seguimiento de Sistemas SCADA, que es el órgano que se encarga de supervisar y controlar todas las actividades y actuaciones que se realicen en los entornos de control de instalaciones.

Las tareas y miembros de este comité están descritos en el documento Norma Organizativa SCADA.

1.4 Excepciones a la Norma Tecnológica SCADA

Toda excepción a la Norma Tecnológica SCADA deberá estar fundamentada en un análisis que demuestre que dicha excepción no tiene impacto funcional negativo sobre el sistema ni sobre las actividades de Aena.

Cualquier propuesta de excepción deberá ser solicitada y aprobada en el Comité de Análisis y Seguimiento de Sistemas SCADA.

1.5 Cláusula de Cumplimiento de la Norma Tecnológica SCADA.

La presente norma será de obligado cumplimiento para todo aquel proveedor, subcontratista, empleado o servicio relacionado con los sistemas SCADA de Aena, que deben comprometerse a cumplir íntegramente las obligaciones que impone a los usuarios de ésta, y que incluye la Norma Tecnológica SCADA, las normas e instrucciones que la complementan y cualesquiera otras que, a nivel local, hayan sido establecidas por la Dirección del Aena en donde vayan a realizar su actividad, y que le serán facilitadas durante la prestación contratada.

Aena se compromete a informar a su personal, y al personal de sus contratas, subcontratas y cualesquier otras empresas o entidades con las que tengan algún tipo de relación contractual o de colaboración de cualquier modificación en la normativa o sus procedimientos. Se incluirá una cláusula al efecto en todos los expedientes administrativos que constituyan o incluyan la construcción de este tipo de sistemas.

1.6 Cláusula de Auditoría.

En el ámbito de la Gestión de la Calidad de la Seguridad o de cualquier otro ámbito de gestión o de regulación aplicable, Aena establecerá auditorías periódicas para comprobar el nivel de desempeño respecto de las normas y metodologías aplicadas, así como del cumplimiento de forma particular de la normativa tecnológica SCADA vigente durante la prestación de los servicios. La periodicidad de dichas auditorías se establecerá en la fase de redacción del proyecto en base a la criticidad del sistema.

Se podrá solicitar la ejecución de acciones correctivas por parte del proveedor sin coste adicional, el cual quedará obligado a la implementación de soluciones eficaces que eliminen las causas que han generado estas no conformidades.

2 Arquitectura del Sistema

2.1 Diseño arquitectura

La Norma Tecnológica SCADA será de aplicación sobre los modelos de desarrollo enumerados en el documento Norma Organizativa SCADA (Punto 3 - Propuesta Organizativa).

Dichos modelos de desarrollo son los siguientes

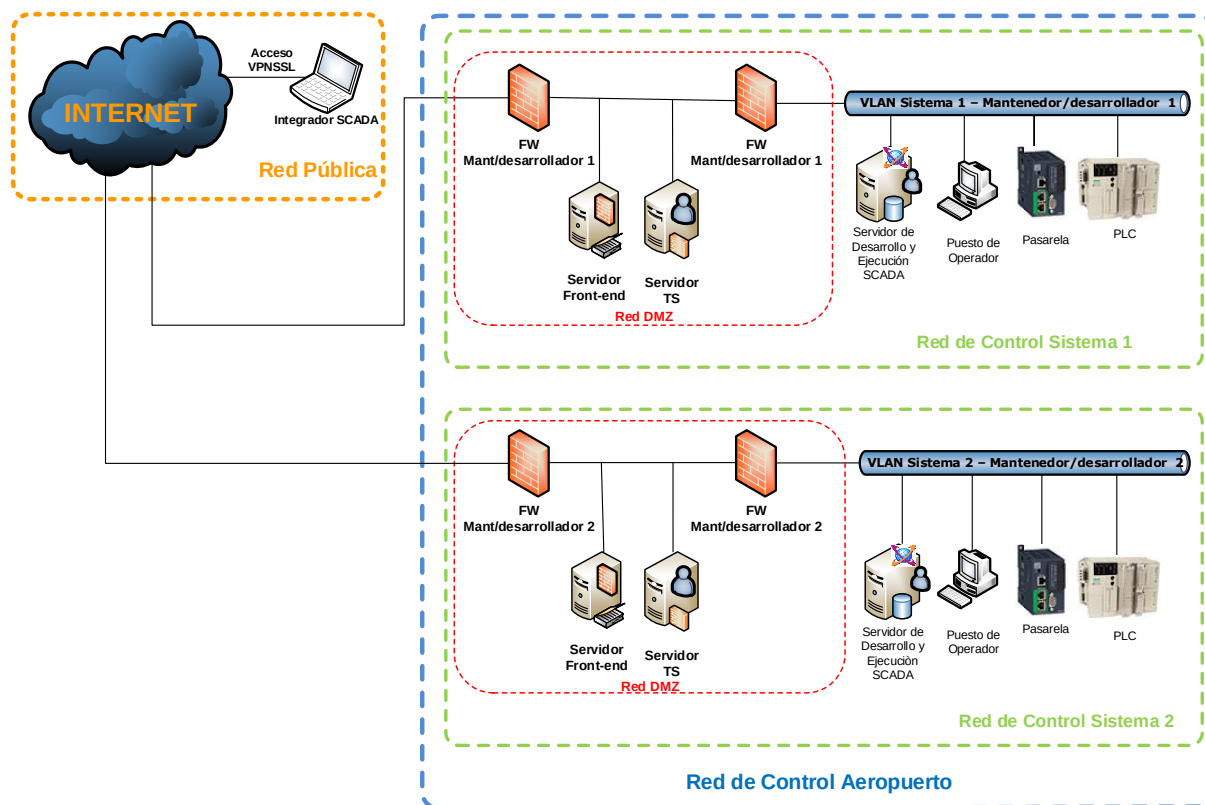
- Modelo de Desarrollo 1: Sistemas SCADA incluidos o no en proyectos de Obra sin participación alguna de la DTIC en ninguno de los niveles. Estos SCADA incluyen un parque de fabricantes extenso y sostenido sobre Software propietario, es decir, no se trata de entornos abiertos sino orientados a fabricantes concretos. La responsabilidad del proyecto recae completamente en el adjudicatario, extremo a extremo, incluyendo todos los componentes TIC que sean necesarios y en su mantenimiento no intervienen las unidades TIC de los aeropuertos ni de SSCC.
- Modelo de Desarrollo 2: Sistemas SCADA DTIC, donde al escenario anterior se añadía la responsabilidad del desarrollo del SCADA junto con el mantenimiento y soporte posterior por parte de la DTIC, es decir un modelo similar al de otros sistemas corporativos. Los elementos de campo y PLC se proporcionaban mediante un expediente aparte del Aeropuerto o en el expediente de la obra correspondiente (salvo en el caso de los Sistemas SCADA de CPD que los proporcionaba la propia DTIC).

Estos modelos de desarrollo se consideran de aplicación a los nuevos sistemas que se implanten en los aeropuertos de la red de Aena, así como también a los sistemas actuales que lo requieran o sufran una modificación/ampliación/actualización.

Para la implementación de los nuevos Sistemas SCADA y las modificaciones/ampliaciones/actualizaciones de los sistemas existentes, se propone una arquitectura de sistema para cada Modelo de Desarrollo (en concreto para el Modelo de Desarrollo 2 se propone una arquitectura con dos variantes, A y B) que, partiendo de las arquitecturas anteriores implantadas en los distintos aeropuertos, añade todos los componentes necesarios para robustecer estos entornos garantizando máxima operatividad y seguridad. Respecto a este último aspecto, se incorpora una capa de seguridad que añade medidas como son la segmentación y separación de redes utilizando tanto soluciones hardware (firewalls) como software (VLANs), proporcionando seguridad ante ciberataques.

2.1.1 Arquitectura para el Modelo de Desarrollo 1

La arquitectura propuesta, de obligado cumplimiento para los nuevos Sistemas SCADA, y a la que deben adaptarse los sistemas actuales incluidos en el Modelo de Desarrollo 1, es la siguiente



Modelo de Desarrollo 1

Donde

Equipo	Nombre	Funcionalidad
 Servidor Front-end	Servidor Front-end	Servidor para el Intercambio de información con usuarios fuera del sistema. En este servidor se sitúan distintos servicios: backups, gestión de usuarios, monitorización, antivirus, etc...
 Servidor TS	Servidor Terminal Services	Operación, mando y control del sistema en estaciones de trabajo no dedicadas
	Servidor de Desarrollo y Ejecución	Servidores de desarrollo, ejecución, , mantenimiento y diagnóstico del sistema
	Puesto de operador	Operación, mando y control del sistema con funcionalidades completas.
	Pasarela / Gateway	Elemento de adaptación de redes industriales a red IP
	PLC / PAC / Remotas	Equipamiento de adquisición de datos, control y automatización.

• En esta arquitectura, la gestión de la conexión a la Red de Control de cada sistema, así como la implementación de la Red DMZ para la securización de los sistemas, es responsabilidad del Mantenedor/desarrollador de dicho sistema. La implementación de la arquitectura se realizará siguiendo las normas establecidas en el presente documento, así como las distintas normas vigentes en el momento de su ejecución, entre ellas:

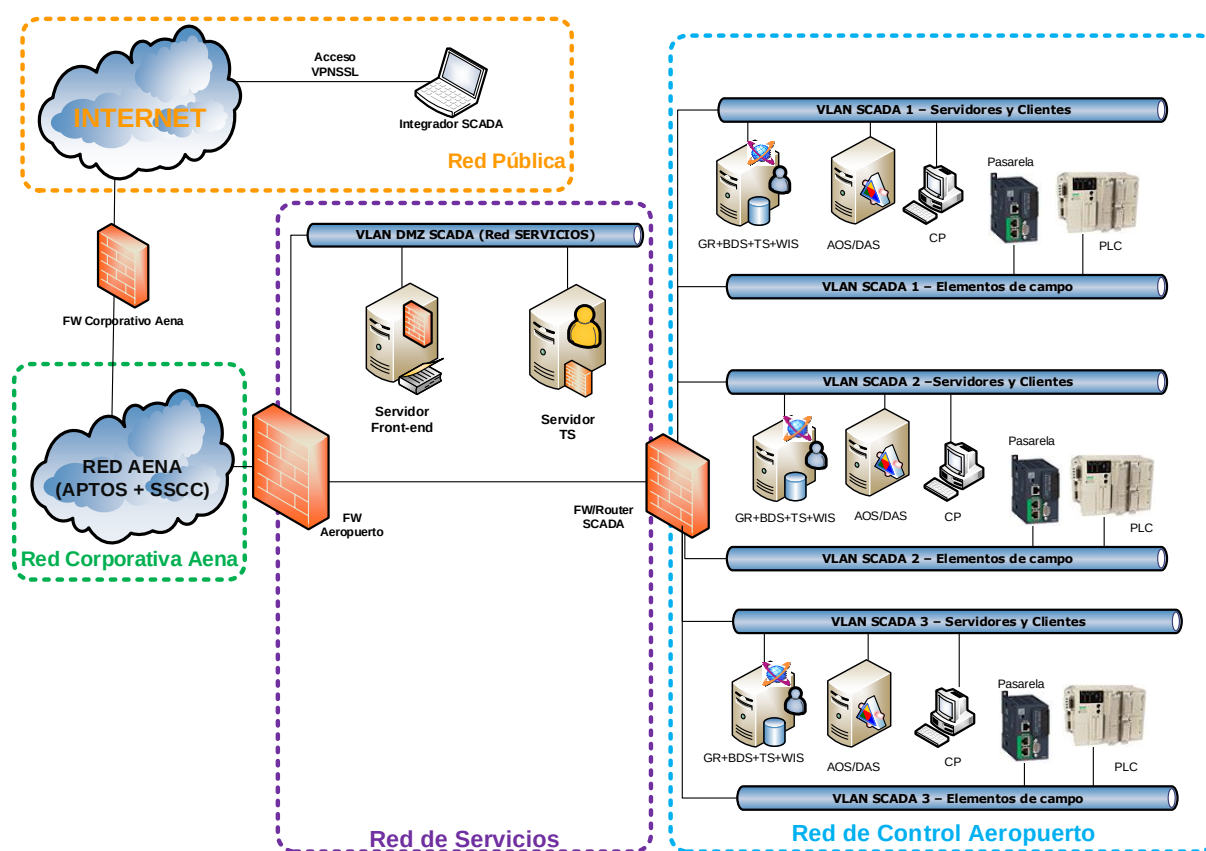
- Norma de Seguridad en entorno de Tecnología Operacional
- Norma Microinformática-Servidores de red.
- Norma interna DTIC de copias de seguridad.
- Norma de monitorización de las aplicaciones.

-
- Norma de Telecomunicaciones
 - Norma de Acceso Remoto.
 - Norma de Desarrollo Seguro de Aplicaciones
 - Norma de Gestión de Parches de Seguridad

2.1.2 Arquitectura para el Modelo de Desarrollo 2

La arquitectura propuesta, de obligado cumplimiento para los nuevos Sistemas SCADA y, a la que se deben adaptar los sistemas actuales basados en el Modelo de Desarrollo 2, tiene dos variantes en función de tratarse de sistemas donde se comparten servidores o no

- Arquitectura Modelo de Desarrollo 2A - Arquitectura de aplicación obligatoria salvo en casos puntuales y adecuadamente justificados y autorizados, en cuyo caso se aplicará la Arquitectura del Modelo de Desarrollo 2 B. En esta arquitectura todos los servidores estarán instalados en la misma red lógica que sus clientes y elementos de campo (PLCs/RTUs/etc.) para evitar latencias en la ejecución y estar lo más aislados posibles. Esta arquitectura será además de aplicación a todos los sistemas críticos de la red de Aeropuertos de Aena.

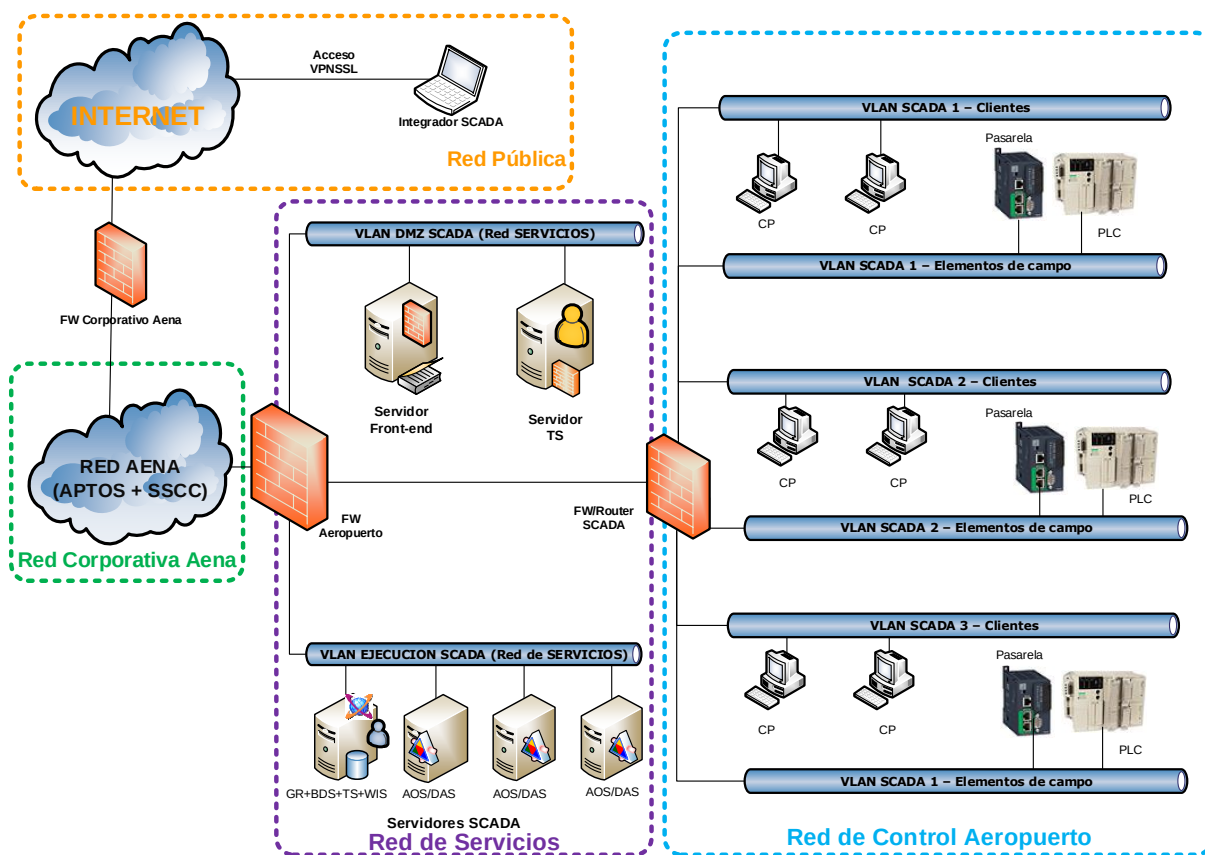


Modelo de Desarrollo 2 A

Donde

Equipo	Nombre	Funcionalidad
 Servidor Front-end	Servidor Front-end	Intercambio de información con usuarios fuera del sistema. Adicionalmente backups gestión de usuarios monitoreo y antivirus
 Servidor TS	Servidor Terminal Services	Operación, mando y control del sistema en estaciones de trabajo no dedicadas
 	Servidor de desarrollo GR+BD+TS+WIS	Desarrollo de aplicación, mantenimiento y diagnóstico. Contiene las funciones de GR, Base de Datos, WIS y Terminal Service.
 	Servidor de ejecución AOS/DAS	Ejecución de lógica y comunicaciones.
 	Puesto de operador CP	Operación, mando y control del sistema con funcionalidades completas.
 	Pasarela / Gateway	Elemento de adaptación de redes industriales a red IP
 	PLC / PAC / Remotas	Equipamiento de adquisición de datos, control y automatización.

- Arquitectura Modelo de Desarrollo 2B - En este caso todos los servidores se instalarán en la red de servicios. Esta arquitectura sólo podrá ser aplicada a los entornos SCADA no críticos y siempre que se implemente la segmentación de redes en la Red de Control, esto es, que no haya comunicación directa entre las diferentes VLANs de la Red de Control desde ningún punto o equipo de la arquitectura.



Modelo de Desarrollo 2 B

Donde

Equipo	Nombre	Funcionalidad
 Servidor Front-end	Servidor Front-end	Intercambio de información con usuarios fuera del sistema. Adicionalmente backups gestión de usuarios monitoreo y antivirus
 Servidor TS	Servidor Terminal Services	Operación, mando y control del sistema en estaciones de trabajo no dedicadas
 	Servidor de desarrollo GR+BD+TS+WIS	Desarrollo de aplicación, mantenimiento y diagnóstico. Contiene las funciones de GR, Base de Datos, WIS y Terminal Service.
 	Servidor de ejecución AOS/DAS	Ejecución de lógica y comunicaciones.
 	Puesto de operador CP	Operación, mando y control del sistema con funcionalidades completas.
 	Pasarela / Gateway	Elemento de adaptación de redes industriales a red IP
 	PLC / PAC / Remotas	Equipamiento de adquisición de datos, control y automatización.

En estas tres arquitecturas se representan las distintas zonas lógicas de red, las interconexiones entre ellas y los distintos componentes que contienen.

La arquitectura de seguridad se basa en los distintos niveles de seguridad definidos en las equivalencias con niveles IEC 62443.

- Red pública: Nivel al que pertenecen las redes no controladas ni confiables. Internet y cualquier otra red cuyo acceso no esté limitado, bien por diseño o bien porque no se controla desde Aena, entra dentro de esta categoría.
- Red Corporativa en Modelo de desarrollo 2: Nivel por defecto de toda red controlada por Aena, y que cumple por tanto con todas las medidas de seguridad Corporativas. Cualquier usuario autenticado en Aena tiene acceso a este nivel.
- Red de Servicios en Modelo de desarrollo 2: Nivel de seguridad perteneciente a la zona desmilitarizada que hace de enlace entre el nivel Corporativo y la Red de Control. Sólo determinados elementos de la Red Corporativa tendrán acceso a esta red. La Red de Servicios tendrá, a su vez, acceso sólo a los elementos y servicios de la Red de Control que sea necesario para el correcto funcionamiento de los sistemas.
- Red de Control: Nivel de seguridad más alto, perteneciente a los Sistemas de control Industrial como PLC, IED, SCADA.

2.1.3 Comunicaciones permitidas

En el modelo de Desarrollo 1, será responsabilidad del Mantenedor/desarrollador del sistema SCADA la gestión de las comunicaciones desde el exterior de la Red de Aena hasta la VLAN correspondiente a su sistema en la Red de Control, tal y como se explica en el punto 2.1.1 Arquitectura Modelo de Desarrollo 1.

Para el Modelo de Desarrollo 2, en la siguiente matriz, leída de izquierda a derecha, se muestran las comunicaciones permitidas entre las diferentes redes, con las siguientes consideraciones

- Desde la Red Pública el acceso está permitido a la Red Corporativa de Aena, las Redes de Servicios de los aeropuertos y a la red de Control, según las consideraciones de seguridad y restricciones descritas en los siguientes párrafos.
- Desde la Red Corporativa de Aena el acceso está permitido a todas las Redes de Servicio de los aeropuertos.
- Desde la Red de Servicios de un aeropuerto el acceso está permitido a la Red de Control de ese aeropuerto y a la red Corporativa. El Acceso no está permitido a Redes de Comunicaciones de otros aeropuertos.
- Desde la Red de Control de un aeropuerto el acceso únicamente está permitido a la Red de Servicios de ese aeropuerto.

	Red Pública	Red Corporativa	Red de Servicios	Red de Control
Red Pública	X	Acceso Estrictamente Controlado	Acceso Estrictamente Controlado	Acceso Estrictamente Controlado
Red Corporativa	X	X	Acceso Controlado	Acceso Controlado
Red de Servicios	Sin Acceso	Acceso Controlado	X	Acceso Controlado
Red de Control	Sin Acceso	Sin Acceso	Acceso Controlado	X

Todos los accesos mostrados en la matriz se realizarán cumpliendo las medidas de protección básica de carácter obligatorio, descritas en los siguientes puntos, que se corresponden con los siguientes niveles de seguridad

- El Acceso Estrictamente Controlado: se realiza a través del canal de acceso remoto seguro establecido por Aena basado en tecnología VPN SSL
- Acceso Controlado: Se tienen que cumplir las medidas de protección básicas de carácter obligatorio descritas en los siguientes puntos, principalmente gobernado por componentes incluidos en una DMZ específica para Sistemas SCADA.

2.1.4 Red de Servicios

La incorporación de la red DMZ en la nueva arquitectura propuesta, tiene como objetivo ubicar los servidores a los que es necesario acceder desde el exterior (Sistemas, Terminal Server, SCADA, etc.) y son precisamente los servicios alojados en estos servidores los únicos que pueden establecer tráfico de datos entre la DMZ o Red de Servicios y la Red de Control.

Por lo tanto, la función de la Red de Servicios, por la que pasará toda comunicación entre Red Corporativa y Red de Control en el modelo de desarrollo 2, es impedir el salto directo desde la Red Corporativa a la Red de Control o al contrario.

Las características y la forma de implementar la Red de Servicios es la siguiente

- La red de Servicios estará dedicada a publicar los servicios de la red de control que deban ser accedidos desde la red corporativa y a ofrecer de manera segura e independiente los servicios de IT a la red de control. Existirá una red de servicios por cada Infraestructura de Control (que a su vez puede estar compuesta por varias Redes de Control diferentes pero relacionadas).
- La red de servicios se encuentra protegida mediante firewalls. Las comunicaciones desde la red corporativa a la red de servicios, quedarán limitadas únicamente a las iniciadas por servidores ubicados en red corporativa con IP fija, y en ningún caso por equipos cliente o con IP dinámica.

Bajo ningún concepto serán permitidas comunicaciones sin filtrar entre la red corporativa y la red de control. Asimismo, no existirá interconexión física entre la red corporativa o la red de servicios y el segmento interno de la red de control (tecnología generalmente propietaria, correspondiente a nivel L1 IEC 62443).

Según la clasificación de criticidad del aeropuerto, se realizará la protección mediante el mismo firewall o distintos firewalls. Para criticidad baja, se puede realizar con un mismo firewall todos los niveles de red. En el caso de criticidad alta, será recomendable el uso de dos firewalls diferenciados. Las dos opciones de configuración serán

- Aeropuerto criticidad alta: La red de servicios (DMZ interna) se define a partir de dos clústeres firewall diferentes. Cuando no sea necesario hacer protección frente ataques (IPS, etc.) se permitirá que el elemento de filtrado de red conectado a los elementos de campo pueda ser un router o switch de nivel 3 con listas de acceso (ACL)
- Aeropuerto criticidad baja: La red de servicios (DMZ interna) se define a partir de un único clúster firewall del aeropuerto.

2.2 Securización

Con el objetivo de mejorar el rendimiento y la seguridad de la arquitectura del sistema se contemplan dos medidas que son la separación y la segmentación de las redes de comunicaciones.

La red IT es una red de datos enfocada a entornos transaccionales, mientras que la red OT, red de control, está pensada para la supervisión, monitorización y operación de procesos industriales. La separación de estas dos redes por lo tanto incorpora mejoras en el tráfico y la seguridad de los datos, no permitiendo que personas sin autorización accedan a zonas restringidas o que el tráfico de datos de distinta naturaleza (protocolos industriales, distinta necesidad de ancho de banda, diferentes necesidades como son la confidencialidad del dato o la disponibilidad de éste, etc.) se “mezcle”.

Segmentar las redes en subredes permite **controlar** el tráfico de forma más efectiva en cada una de las subredes lo que aporta seguridad a la instalación, a la vez que **reducir** el tráfico general de la red mejorando de esta forma el rendimiento de ésta.

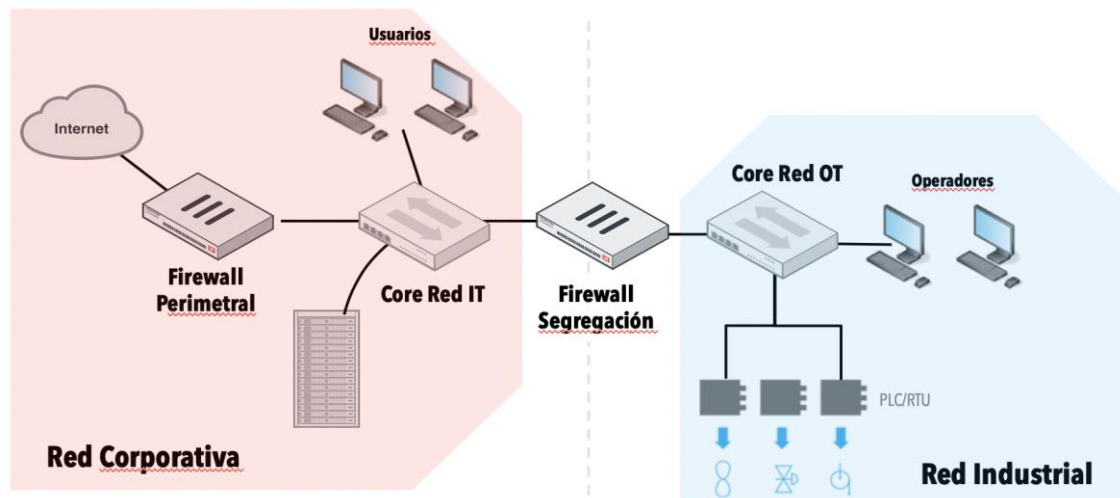
2.2.1 Separación de Redes IT/OT

2.2.1.1 Separación física

El objetivo es la separación completa a nivel físico de las redes IT y OT. Las redes físicas completamente separadas consiguen una separación lógica y física total. Las dos redes se basan en su propia topología de red física. No tienen componentes de red compartidos. Todas las comunicaciones de entrada y salida de la red IT y de las redes OT, se controlan mediante un punto de aplicación de políticas (PaP) de seguridad. Las redes deben estar blindadas de una interfaz a otra.

Esta solución también aporta la ventaja de que las áreas separadas se pueden desarrollar de manera diferente. Por consiguiente, en cualquier migración de cualquiera de las dos redes, sólo es necesario modificar el elemento de acoplamiento (punto de aplicación de políticas (PaP) de seguridad) para garantizar la comunicación entre las áreas.

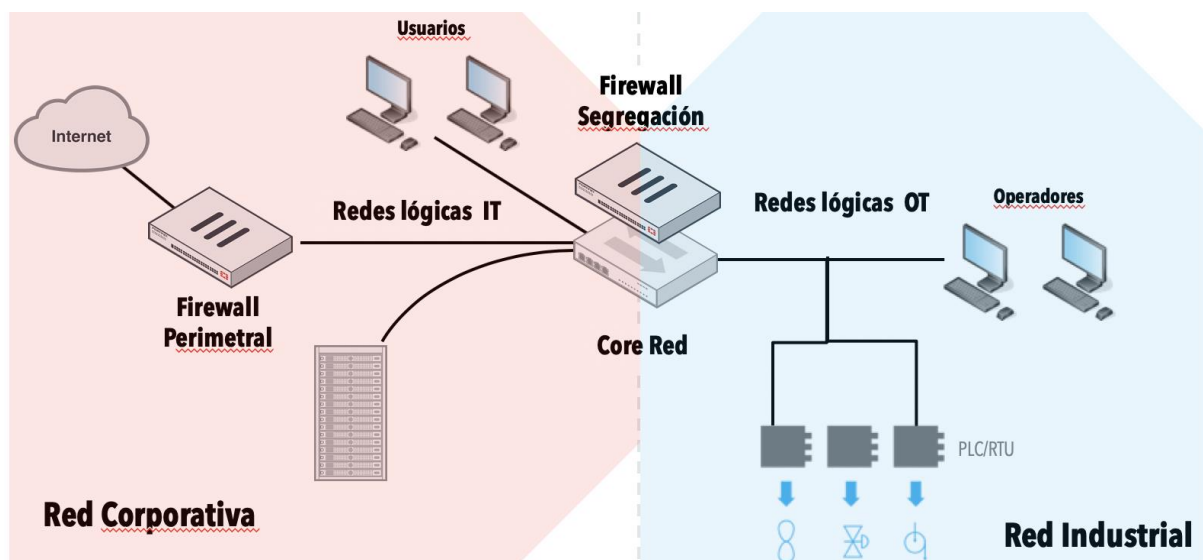
Teniendo en cuenta el ciclo de vida tan diferente de ambas redes de comunicaciones (el ciclo de vida de la red OT es muy superior al ciclo de vida de la red IT debido a las distintas naturalezas de dichas redes), así como el desarrollo más rápido de la red IT, la separación física de las redes es un hecho positivo ya que permite la vinculación de diversas etapas de desarrollo técnico de la red.



2.2.1.2 Separación Lógica

Esta solución es de aplicación en aquellos sistemas correspondientes al modelo de Desarrollo 2 donde no sea factible aplicar la separación física de redes.

En esta solución, la misma infraestructura física de red es utilizada tanto por la red IT como por la red OT. La separación es lógica y se basa en la creación de VLANs de red en la capa 2, siendo los Firewalls los encargados de las comunicaciones básicas entre las redes. Dentro de la red de control las comunicaciones son gestionadas mediante un punto de aplicación de políticas (PaP) de seguridad.



2.2.2 Segmentación de Redes OT

La segmentación de redes se realiza con el objetivo claro de contener amenazas y evitar su propagación dentro de la red de control (OT). Este método consiste en la división de una red en subredes (zonas de seguridad) de forma que la comunicación entre dichas subredes sólo se realiza cuando es necesario y cumpliendo unos requisitos de seguridad determinados.

2.2.2.1 Acceso desde el Exterior

a) Modelo de Desarrollo 1

Será responsabilidad del Mantenedor/desarrollador del sistema SCADA la gestión de las comunicaciones desde el exterior de la Red de Aena hasta la VLAN correspondiente a su sistema en la Red de Control, tal y como se explica en el punto 2.1.1 Arquitectura Modelo de Desarrollo 1.

b) Modelo de Desarrollo 2

Respetando los principios generales de la arquitectura propuesta y la estrategia de seguridad en profundidad, el acceso desde el exterior a la Red de Control utilizará diferentes servicios, situados tanto en nivel Red Corporativa como Red de Servicios.

Los distintos servicios se agrupan de la siguiente manera

- **Terminal VPN:** se emplaza en la Red Corporativa y es la única máquina desde la que se permite acceder al Terminal Server Genérico Securizado DMZ. Esta máquina estará publicada en el portal de acceso VPNSSL.
- **Terminal Server Genérico Securizado DMZ:** recibe conexiones procedentes de la máquina Terminal VPN. Tiene visibilidad sobre el interfaz web del aplicativo. Este Terminal puede tener directivas de grupo (GPO) para definir los usuarios que pueden entrar desde la Terminal VPN.
- **Aplicativo:** localizado en la Red de Servicios, realiza las funciones necesarias sin exponer ningún interfaz a la Red Corporativa directamente.

El acceso externo se realizará desde la VPN SSL de Aena, mediante un portal publicado en Internet. Tras la correcta autenticación del usuario este portal proveerá de acceso directamente a una red o equipos individuales según los privilegios asociados al usuario.

Los requisitos y el nivel de seguridad para acceder a la Red Corporativa para usuarios externos a Aena deberán cumplir la política de seguridad corporativa.

El usuario que necesite acceder a la Red de Control y se haya autenticado correctamente en el portal de internet, dará dos saltos, siendo el segundo de ellos tan transparente al usuario como permita el recurso de acceso:

- Autenticación en la VPN SSL a través del portal publicado en Internet, para entrar en la Red Corporativa de Aena.
- Acceso al Terminal Server Genérico Securizado situado en la VLAN DMZ SCADA (Red Servicios)
- Acceso desde Terminal Server Genérico Securizado al aplicativo instalado en Red de Control

2.2.2.2 Redes de control de diferentes proveedores / tecnologías

Cuando en una red de control coexistan sistemas de diferentes proveedores o tecnologías, que no cumplan con los requisitos de seguridad de la organización, que sean incompatibles entre sí o que sea recomendable su separación, se deberá proporcionar un nivel de aislamiento adecuado para evitar que los sistemas interfieran. Para ello será necesaria la creación de VLANs consideradas a priori del mismo nivel de seguridad, equivalente al nivel de Red de Control.

Los criterios a seguir para la creación de estas VLAN son los siguientes:

- Switch de acceso: Los elementos que integren una VLAN no pueden concurrir con los de otra VLAN en switches a nivel de acceso. Es decir, un switch de acceso se considerará perteneciente a una VLAN concreta, nunca a más de una.
- Access Control List (ACL): En los casos que el enrutamiento entre redes (nivel 3) no lo realice un Firewall, se realizará filtrado de conexiones mediante el uso de Access Control List (ACL).
- Uso de VLAN: Los distintos componentes de los Sistemas SCADA se instalarán en redes separadas (VLAN) según su función. Desde las diferentes VLAN estarán accesibles los servidores de la Red de Control (DC, WSUS, ...). El propósito es evitar la interferencia entre diferentes subsistemas. Por ejemplo, si la subred de un proveedor ve comprometida su seguridad y comienza a realizar broadcast masivo, no es deseable que sature la red de otro proveedor o que simplemente provoque un consumo de CPU en su sistema. Con la separación propuesta se evitan interferencias innecesarias entre sistemas distintos.
- Cumplimiento europeo niveles ISA-99 / IEC62443: Las redes de un proveedor concreto, en general, contienen todos los niveles descritos en ISA99 y constituyen un subsistema de control completamente funcional. Como se ha comentado estas redes deben separarse entre sí para no interferir en condiciones normales de trabajo y en especial en caso de sufrir accesos no autorizados.
- Equipos Legacy: En el caso de que sea necesario integrar la red de un proveedor con equipos Legacy en las redes de Aena, se utiliza un servidor aislado en una VLAN diferente y se conecta a la red del proveedor mediante un equipo de interconexión de capa 3 (enrutador). De esta forma en caso de existir tráfico masivo no deseado (ej.: DDoS), éste quedaría confinado a esa subred sin escalar al resto de la infraestructura. En caso de querer proteger estos equipos Legacy, el equipo de interconexión será un Firewall con protección de ataques conocidos (IPS, etc.).

2.2.2.3 Acceso desde una red pública

Toda red pública (incluida internet) se considera un nivel de seguridad diferente e inferior al nivel de Red Corporativa, por lo que no se permite el acceso directo desde una red pública, salvo las conexiones permitidas desde el acceso corporativo VPNSSL de Aena.

Los casos de comunicación lógica que representen una omisión de alguna de las conectividades físicas representadas, como el uso de túneles o proxies, se tratarán como casos excepcionales, siendo obligatorio ser conocidos y validados por el Comité de Análisis y Seguimiento de Sistemas SCADA (o en quien el comité delegue) antes de su implementación.

2.2.2.4 Firewalls para segmentación específica del Sistema de Control Industrial

Los firewalls necesarios para la segmentación y control de acceso a una red específica del Sistema de Control Industrial deben tener abiertos únicamente los puertos en uso por el sistema y denegar el tráfico restante. Cuando estos firewalls sean aportados por el adjudicatario del sistema a implantar, la configuración de los mismos debe ser validada por Aena como paso previo a su puesta en servicio. Su administración y gestión serán responsabilidad de dicho adjudicatario.

2.2.2.5 Niveles de red, zonas, conductos y canales definidos en el estándar IEC 62443

Los niveles de red dentro de esta norma están derivados y alineados con el estándar ISA99 para la integración de los sistemas de control y el estándar IEC 62443 para la seguridad de los mismos.

El estándar IEC62443 introduce el concepto de “zonas” y “conductos” como una manera de segmentar y aislar los distintos subsistemas en una red de control. Se definen como:

- Una zona se define como un conjunto de activos físicos o lógicos que comparten aspectos comunes en cuanto a la seguridad tales como la criticidad.

- Un conducto se define como la ruta de información que fluye entre dos zonas y que debe proveer las funciones de seguridad necesarias para la comunicación entre ellas.
- Un canal se define como un conjunto de conductos por tanto y a diferencia de un conducto, un canal puede establecerse entre más de dos zonas.

La identificación de zonas requiere el análisis inicial de las instalaciones y la agrupación de elementos en base a una funcionalidad y unos requisitos de seguridad comunes. Siguiendo las recomendaciones sobre ciberseguridad industrial, se diferenciará entre 5 capas de seguridad, desde la capa de nivel 4 hasta la capa de nivel 0.

La clasificación de los niveles viene de menor nivel de seguridad (Nivel Seguridad 4) a mayor nivel de aislamiento y seguridad (Nivel Seguridad 0).

Los niveles de seguridad de la red en un entorno de tecnología de la operación siguiendo la estructura actual de Aena sería la siguiente:

- Nivel Seguridad 4 – Red Corporativa Aena (Modelo de desarrollo 2)
 - Nivel 4.1 – Red RECOA (Modelo de desarrollo 2)
- Nivel Seguridad 3 – Red de Servicios DMZ de acceso a OT
- Nivel Seguridad 2 – Red SCADA
- Nivel Seguridad 1 – PLC, IED, RTU,
- Nivel Seguridad 0 – Sensores y actuadores

La red RECOA será considerada una red corporativa interna de Aena. Debido a la cantidad de conexiones a la que es sometida, una vulnerabilidad en un aeropuerto puede permitir el salto a otro aeropuerto. Por lo tanto, esta red deberá estar separada de los aeropuertos por un firewall que filtre la entrada y salida de comunicaciones, aislando así cada aeropuerto.

Cualquier conexión de entrada a las redes de control industrial de Aeropuertos siempre pasará a través de un servidor TS securizado y auditado, instalado en la red de Servicios DMZ.

En las redes de 'Nivel Seguridad 1 (PLC, RTU, etc.)' cuya complejidad por número y tipo de elementos sea elevada, se segregarán en diferentes redes lógicas de la siguiente forma:

- Red de Servidores/Clientes
- Red de Elementos de recolección de señales de campo (PLC/RTU/etc.)
- Cámaras
- Elementos de gestión de red (switches)

Los componentes de la Red de Control (PLC, sensores, etc.) tienen prestaciones TIC moderadas, no disponiendo de un nivel suficiente de monitorización y parchado de vulnerabilidades. Además, el número y tipo de tecnologías de los elementos de dicha red (OT) es muy numeroso siendo el parque de fabricantes bastante extenso.

Por el contrario, los elementos que componen la Red de Servicios son de alto nivel de prestaciones TIC, y están en el máximo nivel de monitorización y parchado de vulnerabilidades. Los fabricantes aportan soluciones de parcheo en pocos días ante la detección de anomalías. Adicionalmente el número y tipo de tecnologías que componen la Red de Servicios es reducido.

Estas circunstancias obligan a incorporar un nivel más de seguridad a la Red de Control con respecto de la Red de Servicios.

2.2.2.6 Consideraciones de la arquitectura de red de control industrial

La Red de Control Industrial tendrá un diseño de red multicapa de manera que permita contemplar los siguientes conceptos, proporcionando una escalabilidad que va a permitir una futura expansión.

- Jerarquía: La jerarquía es una caracterización del flujo del tráfico a través de la red, que implica que el flujo crezca pasando a través de puntos de agregación (nodos) y que tienda a seguir unas direcciones y patrones específicos.
- Modularidad: La red estará compuesta de distintos bloques, cada uno de ellos con sus propias características y comportamientos. La modularidad también implica aislamiento; los diferentes bloques están separados e interactúan a través de mecanismos específicos simplificando el control y la seguridad. Cada uno de ellos es independiente de los demás y los cambios en un bloque no afectan a ningún otro.
- Escalabilidad: La red deberá poder crecer considerablemente sin realizar cambios drásticos ni tener que realizar un rediseño de la red. Es una consecuencia directa de la jerarquía y de la modularidad.
- Tolerancia a fallos: Deberá realizarse un diseño de red con redundancias que permita que el sistema siga funcionando ante el fallo de uno de los componentes.
- Previsibilidad: El comportamiento del flujo del tráfico será fácilmente representado, los retardos predecibles con márgenes razonables y los enlaces de backup fácilmente identificables.
- Simplicidad: El diseño será lo más simple posible eliminando todos los enlaces y funcionalidades que no sean estrictamente necesarios.

2.3 Requisitos de Ingeniería de Sistemas de Control

2.3.1 Arquitectura Software

La arquitectura software de los Sistemas de Control, tendrá la siguiente división de tareas y funciones basada en capas, con caracterización según tecnologías. Este criterio de arquitectura será de obligado cumplimiento para todos los desarrollos nuevos o modificaciones que se acometan en Sistemas SCADA.

Resumidamente se utilizarán las herramientas SCADA para la *monitorización*, los PLC para la *automatización y control de procesos* y las RTU para la *captura de información*.

Nivel SCADA/HMI

- Monitorización de procesos
- Diálogo hombre-maquina
 - Ajustes
 - Selección modos de funcionamiento
 - Configuración escenarios de funcionamiento
 - Etc.
- Monitorización y gestión de alarmas y eventos
- Historización de variables, alarmas y eventos
- Informes
- Lógica de agregación de información

Nivel PLC/PAC

- Lógica de automatización
- Lógica de regulación y control
- Lógica de captura de información

- Lógica de funcionamiento de modo degradado
- Lógica de alarmas severas (paro/disparo)

Nivel RTU/DataLogger

- Captura de información
- Datado de información
- Agregación de información

No se utilizarán las tecnologías para funciones fuera de las propuestas. A modo de ejemplo, no estará permitido usar scripting en los sistemas SCADA para controlar procesos.

2.3.2 Redundancia

Se utilizarán arquitecturas redundantes en los equipos de control (PLC/PAC) que estén a cargo de procesos críticos para la operatividad aeronáutica (balizamiento, energía).

Se podrán usar configuraciones redundantes gestionadas tanto por hardware especializado, como por software empotrado en ellos sistemas.

Se utilizarán arquitecturas redundantes en los sistemas de monitorización (SCADA) en todos los casos.

2.3.3 Tecnologías

En general para avalar la solvencia de la tecnología propuesta, Aena se reserva el derecho de comprobar en el Centro de Respuesta a Incidentes de Seguridad INCIBE-CERT, operado conjuntamente por INCIBE (Instituto Nacional de Ciberseguridad) y CNPIC (Centro Nacional de Protección de Infraestructuras y Ciberseguridad) que dicha tecnología no presenta ninguna vulnerabilidad que pueda afectar negativamente a la operación y mantenimiento del sistema a implantar en la red de aeropuertos de Aena, listada en los avisos de seguridad de Sistemas de Control Industrial (SCI), y no resuelta.

Además

- *Las tecnologías usadas en la capa de monitorización (SCADA)* serán de tipo comercial, ampliamente implantadas y reconocidas, con referencias en el ámbito aeroportuario, con una red de integradores, planes de formación y planes de soporte.
- Se deberá acreditar la solvencia técnica mediante la presentación de los requisitos anteriores, y no se permitirán soluciones a medida que no estén suficientemente contrastadas. Serán necesarias referencias, planes de formación y planes de soporte.

Cualquier desarrollo realizado por un integrador sobre una solución de mercado, deberá poderse continuar por otro integrador distinto. No se permitirán programaciones con módulos no abiertos ni documentados (tipo caja negra) o utilizando kits de desarrollo que oculten u ofusquen la programación.

En todo caso, se dará preferencia al uso del software corporativo de Aena.

- *Las tecnologías usadas en la capa de control y adquisición (PLC/PAC)* serán de tipo comercial, ampliamente implantadas y reconocidas, con referencias en el ámbito aeroportuario, con una red de integradores, planes de formación y planes de soporte.

Se deberá acreditar la solvencia técnica mediante la presentación de los requisitos anteriores, y no se permitirán soluciones a medida que no estén suficientemente contrastadas. Serán necesarias referencias, planes de formación y planes de soporte.

Cualquier sistema desarrollado por un integrador sobre una solución de mercado, deberá poderse continuar por otro integrador distinto. No se permitirán programaciones con módulos

no abiertos ni documentados (tipo caja negra) o utilizando kits de desarrollo que oculten u ofusquen la programación.

- Las redes que den soporte a las tareas de regulación y control deberán tener capacidades de funcionamiento determinista. En función del proceso que se aborde, se definirá el nivel de exigencia en los tiempos de respuesta

2.3.4 Gestión de alarmas y eventos

El sistema registrará la fecha, hora y valor que originó la alarma cuando suceda una nueva. De igual manera se hará con el momento de desaparición de la condición de alarma, y de la acción de reconocido por parte del operador.

En la pantalla de representación de general del proceso/planta, se indicará con un cartel de FALLO parpadeante, la ubicación del subsistema o subsistemas en los que ha aparecido la alarma o alarmas.

Es posible que existan otras alarmas activas, pero reconocidas con anterioridad, mostrándose con el cartel de FALLO sin parpadeo.

El operador podrá entrar a ver un detalle de las alarmas ocurridas en ese subsistema pulsando sobre el cartel de FALLO. Allí encontrará toda la información disponible acerca de esta alarma, así como de la posibilidad de ver los eventos relacionados con este subsistema y el acceso al detalle de otros subsistemas.

2.3.5 Navegación por la aplicación

La navegación por la aplicación será totalmente intuitiva, necesitando que el único conocimiento de informática del operario sea el correcto uso del ratón. Se prescinde completamente del teclado mecánico.

El usuario se moverá por el sistema, identificando perfectamente los elementos. Siempre tendrá completo conocimiento de qué zonas de las pantallas son accesibles, ya que el sistema las presentará en forma de tecla/botón.

Todo el diseño de accesos a pantallas, infografía y presentación de datos se hará buscando una aplicación intuitiva y ergonómica, prescindiendo de terminología eminentemente informática y enfocando al sistema hacia las necesidades del sistema/proceso a operar.

2.4 Requisitos del sistema de control SCADA

2.4.1 Disponibilidad del Sistema SCADA.

Los Sistemas SCADA implantados en Aena deben ser sistemas en Alta Disponibilidad, ello implica que el sistema debe funcionar correctamente ante el fallo de cualquier nodo servidor o cliente, mientras el fallo solo se produzca en uno simultáneamente. Los sistemas deben diseñarse acordes a este requerimiento.

Para ello es necesario aplicar medidas de redundancia a las aplicaciones, a los servidores y a las comunicaciones para evitar pérdidas de información durante la caída de un equipo de comunicaciones, servidor o base de datos.

Existen excepciones inherentes a determinadas funcionalidades del sistema que no tienen por qué tener alta disponibilidad, como pueden ser: los informes, las consultas de alarmas históricas y consulta de datos históricos, etc...

2.4.2 Planificación de recuperación del sistema

Con el objetivo de realizar una planificación de recuperación del sistema, previa a la instalación de un nuevo Sistema SCADA, el adjudicatario deberá documentar los procedimientos para realizar una copia de seguridad incremental y completa y la restauración/recuperación del Sistema SCADA y los datos.

Los Sistemas SCADA se configurarán para realizar automáticamente una copia de seguridad de la base de datos de control, la configuración del sistema y otra información vital en el disco duro como mínimo una vez por semana.

Se debe almacenar fuera de línea un mínimo de dos conjuntos de datos completos de copia de seguridad y recuperación para cada estación de trabajo, servidor y RTU.

Se debe realizar una copia de seguridad completa del sistema en todas las instalaciones nuevas de equipos SCADA.

Esto incluye el sistema operativo y los archivos de configuración.

- La copia de seguridad debe ser probada y verificada.
- se hacen dos copias de la copia de seguridad. Una copia se almacenará en una ubicación segura en el sitio y la otra copia se mantendrá en un lugar seguro fuera del sitio.

El Sistema SCADA se configurará para almacenar la copia de seguridad en línea en una unidad de disco duro diferente al del Sistema SCADA del que se está haciendo la copia de seguridad.

El equipo de control del proceso que contiene almacenamiento de datos debe ser limpiado de acuerdo con el procedimiento antes de su eliminación.

Todas las cuestiones relacionadas con la alta disponibilidad, así como las medidas tecnológicas necesarias para llevar a cabo un Plan de Recuperación de Desastres (PRD) de las aplicaciones, servidores y comunicaciones, utilizada para implementar la red de servicios, deberán ser analizadas y definidas en base al análisis de riesgos realizado para cada despliegue concreto.

2.4.3 Seguridad y acceso al sistema.

Para todos los Sistemas SCADA será de cumplimiento lo establecido en el punto “3.2.2.1.4 Protección de Acceso” de este documento.

Además, para los Sistemas SCADA desarrollados con tecnología Wonderware será de obligado cumplimiento lo establecido en cuanto a seguridad y acceso al sistema en los siguientes documentos:

- Documento Norma de Seguridad de la DTIC para el desarrollo seguro de aplicaciones:
- https://gdtic.aena.es/normas/seguridad/SEGURIDAD%20LOGICA/Norma_Desarrollo_Seguro_Aplicaciones_v5.pdf
- Documento Checklist Desarrollo Seguro:
- https://gdtic.aena.es/normas/seguridad/SEGURIDAD%20LOGICA/Checklist_desarrollo_seguro.xlsx
- Estándares de diseño Aena SCADA:
[https://gdtic.Aena.es/normas/Lists/Normas%20SCADA/Attachments/14/Estándares%20de%20Diseño%20Aena%20-%20Wonderware%20\(4.0\).pdf](https://gdtic.Aena.es/normas/Lists/Normas%20SCADA/Attachments/14/Estándares%20de%20Diseño%20Aena%20-%20Wonderware%20(4.0).pdf)

Todos los perfiles operacionales deberán ser definidos en los requisitos del sistema por el responsable funcional del Sistema SCADA. Dichos perfiles y los usuarios de acceso deberán ser gestionados desde el dominio. Cualquier otro tipo de gestión de usuarios deberá ser aprobado por el Comité de Análisis y Seguimiento de Sistemas SCADA (CASS).

Además de cara a implantar desarrollos seguros, para cualquier Sistema SCADA desarrollado para Aena, sea cual sea la tecnología utilizada, deberán quedar totalmente documentados los puertos de comunicación que utilice el software, ya sea de la propia solución base utilizada, como del propio desarrollo implementado y sus elementos de comunicación con campo.

2.4.4 Documentación exigida

Para todos los desarrollos SCADA de Aena será necesario entregar, como mínimo, la siguiente documentación:

- Manual de Instalación del Sistema SCADA
- Manual de usuario del Sistema_SCADA
- Documento de Diseño Técnico del Sistema (DTS)
- Backup completo del desarrollo
- Listado y documentación técnica de los equipos monitorizados
- Listado y documentación técnica de los equipos proveedores de datos de entrada/salida utilizados (PLCs, remotas, pasarelas, tarjetas de comunicaciones, etc.)
- Esquema y descripción de la red de campo implementada (incluyendo elementos de campo y elementos monitorizados) y puertos de comunicación
- Programación de PLC, ficheros de configuración necesarios para los elementos de campo y fichero de texto plano con credenciales de acceso a todos los elementos proveedores de datos.

Los desarrollos de Sistemas SCADA realizados con la solución corporativa elegida por Aena deberán regir sus entregas según lo indicado en el documento del enlace siguiente

[https://gdtic.Aena.es/normas/Lists/Normas%20SCADA/Attachments/15/Documentación%20a%20entregar%20y%20requisitos%20\(6.0\).pdf](https://gdtic.Aena.es/normas/Lists/Normas%20SCADA/Attachments/15/Documentación%20a%20entregar%20y%20requisitos%20(6.0).pdf).

3 Seguridad aplicada a los sistemas SCADA

La seguridad de los Sistemas SCADA es especialmente relevante cuando se ven afectadas instalaciones y sistemas que son claves para correcto funcionamiento de la infraestructura donde se encuentran. En este punto, se establecen los requisitos y directrices que se deberán seguir para proporcionar un marco de protección para los Sistemas SCADA de Aena.

Se consideran los siguientes puntos

- Requisitos de Seguridad
 - General- requisitos aconsejados por las leyes y estándares de aplicación a los desarrollos, sistemas y redes de comunicaciones de los sistemas de control.
 - Cumplimiento de las leyes territoriales e internacionales- son las leyes que se deberán cumplir/tener en cuenta en la nueva implementación o modificación/actualización de los Sistemas SCADA.
 - Responsabilidades y Obligaciones- Hace referencia a las obligaciones en materia de seguridad de los sistemas de información para todos los usuarios de Aena y colaboradores.
 - Interlocutor válido en ciberseguridad- figura solicitada al desarrollador y mantenedor en los proyectos SCADA con la finalidad de garantizar el cumplimiento de las medidas de seguridad establecidas en la presente normativa.
- Estudio de seguridad
 - Análisis de Riesgos
 - Medidas de protección básica- son las medidas que se deberán llevar a cabo en cada tipo de control, definiendo estos tipos de control como, técnico-globales y operativos.

3.1 Requisitos de seguridad

3.1.1 General

El presente documento se ha elaborado teniendo en cuenta los Requisitos de Seguridad en un entorno industrial de desarrollo, tanto a nivel compliance como técnicos, recogidos en el documento *Checklist desarrollo seguro v9.0* basado en el marco de buenas prácticas propuesto en la última publicación del NIST Special Publication 800-53 revisión 5.

Estos requisitos, presentados por el estándar, han sido completados y mapeados con los controles propuestos en el estándar específico de Sistemas de Control Industrial de la NIST Special Publication 800-82 revisión 2 y el estándar europeo IEC62443-3-3, que recoge los requisitos de seguridad en las redes de comunicación industrial.

La arquitectura de seguridad para entornos SCADA de Aena es la recogida en punto 2 del presente documento.

3.1.2 Cumplimiento de las leyes territoriales e internacionales

Además de las leyes mencionadas en otros puntos, se deberá cumplir/tener en cuenta las siguientes:

- El Reglamento General de Protección de Datos (en adelante, RGPD) que entró en vigor el pasado 25 de mayo, será de aplicación obligada el 25 de mayo de 2018. Este “vacatio legis” permite a los sujetos obligados y a los Estados Miembros, a adaptar sus organizaciones y legislaciones nacionales a los requisitos y obligaciones establecidos en dicho Reglamento; mientras tanto, la Directiva 95/46/CE y nuestra normativa nacional, es decir la LOPD y el

RLOPD, permanecerán en vigor y plenamente aplicables hasta el 25 de mayo de 2018, fecha en la que la Directiva quedará derogada. Por lo tanto, cuando se manejen datos de carácter personal, se debe incluir los controles que forman parte de los requisitos de seguridad de tipo funcional del RGPD y de la LOPD.

- El real decreto- ley 12/2018 (Directiva NIS), de 7 de septiembre busca mejorar el nivel de seguridad de las redes y sistemas de información en la Unión Europea, estableciendo requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales, a los que insta a adoptar las medidas oportunas para gestionar los riesgos en seguridad y notificar los incidentes que tendrían un efecto perturbador significativo a las Autoridades Nacionales Competentes, proponiendo la creación de una red de cooperación entre todos los diferentes Estados Miembros.
- La actual legislación de Infraestructuras Críticas- Ley 8/2011- establece que los Operadores Críticos deben proteger frente a ataques o desastres que afecten gravemente a los servicios públicos ofrecidos, garantizando con ello en todo momento un nivel servicio necesario para el orden público y la defensa de la seguridad nacional.
- Se desarrolló un reglamento y unas guías para que los operadores puedan determinar qué infraestructuras y servicios bajo su responsabilidad deben protegerse especialmente.
- Hasta la fecha, las guías que más impactan directamente sobre el desarrollo son las guías de Sistemas SCADA desarrolladas por el CCN. En el caso de Aena, deben protegerse los servicios que dan soporte al normal funcionamiento de aeropuertos, asegurando la operatividad de los mismos.

En cualquier caso, cualquier aplicación que se determine como crítica desde el punto de vista de esta ley deberá cumplir con unos requisitos mínimos de seguridad.

- CCN-STIC-480-Guía de seguridad de las TIC-Seguridad en Sistemas SCADA.
- ISO 27001- information security management systems requirements.
- ISO-27002-Code of practice for information security controls.
- ISA 99
 - ISA-62443-2-1: IACS security management system – Requirements.
 - ISA-62443-2-2: IACS security management system – Implementation guidance

3.1.3 Responsabilidades y obligaciones

Obligaciones en materia de seguridad de los sistemas de información para todos los usuarios de Aena y colaboradores

- Respetar, asumir y ejecutar las obligaciones o acciones pertinentes y necesarias que se deriven de la Política de Seguridad de la Información vigente en Aena, en base a las recomendaciones de la Norma UNE-ISO/IEC 27002:2013 "Código de buenas prácticas para la Gestión de la Seguridad de la Información", así como el resto de directivas de seguridad, normativas, etc., que se desarrollen o ejecuten en el ámbito de Aena, con la finalidad de garantizar la seguridad de los Sistemas de Información de Aena, y de los datos e informaciones a los que tenga acceso para la ejecución del objeto del presente contrato, siempre y cuando las mismas sean notificadas por escrito y con antelación a la Empresa Adjudicataria y no supongan un incremento económico.
- La adopción de dichas acciones o medidas implica, no sólo el respeto y adaptación a las medidas, controles y procedimientos de Aena, sino también la garantía, y en su caso adopción de las medidas de seguridad necesarias en los propios Sistemas de Información de la Empresa Adjudicataria o contratista, que garanticen a Aena que dicha entidad cumple u ostenta un

estándar mínimo de seguridad. Dichas normas y medidas serán proporcionadas por Aena a la empresa adjudicataria.

Según lo establecido en el Real Decreto-ley 12/2018, de 7 de septiembre, Aena tiene la obligación de notificar los incidentes que puedan tener efectos perturbadores significativos sobre la integridad y disponibilidad de los servicios prestados al ciudadano, así como sobre la confidencialidad de la información que se maneja. La notificación tiene un carácter preventivo, pues basta con que el incidente se produzca para que surja la obligación de notificación, aunque el efecto adverso aún no sea real.

Además de las notificaciones del incidente, también es necesario notificar su resolución (notificación final) y cualquier otra información que afecte a su evolución mientras no esté resuelto (notificaciones intermedias). Las notificaciones de los incidentes de seguridad se realizarán según lo descrito en el punto 3.7 “Delegación y Soporte” de este documento.

En todo caso, se deberá cumplir con las políticas, normas y procedimientos vigentes y aquellas que pudieran aprobarse, entre las cuales cabe citar las siguientes:

- Política de Seguridad de la Información
- Política de acceso a red de datos y uso de activos informáticos.
- Política de accesos a internet.
- Política de Clasificación de la Información.
- Política de Uso del Correo electrónico corporativo.
- Política de Gestión de Cambios.
- Política de Gestión de usuarios en las aplicaciones.
- Política de Acceso Remoto

Adicionalmente, los entornos de los sistemas de control industrial, donde aplique, deberán alinearse con las Normas y Procedimientos vigentes y aquellos que pudieran aprobarse, entre los cuales cabe citar las siguientes:

- Norma de Seguridad en entorno de Tecnología Operacional
- Norma Microinformática-Servidores de red.
- Norma interna DTIC de copias de seguridad.
- Norma de monitorización de las aplicaciones.
- Norma de Telecomunicaciones
- Norma de Acceso Remoto.
- Norma de Desarrollo Seguro de Aplicaciones
- Norma de Gestión de Parches de Seguridad

Los sistemas de control industrial deberán atender todas las auditorías a las que Aena se vea sometida.

3.1.4 Interlocutor de Seguridad.

Con la finalidad de garantizar el cumplimiento de las medidas establecidas en la presente normativa, se establece que cada proveedor o participante en proyectos relacionados con el entorno de los Sistemas SCADA de Aena deberá definir y disponer de un interlocutor principal de gestión para las tareas de Ciberseguridad.

El Interlocutor será el responsable de garantizar que el proyecto, suministro y/o empresa cumple con las normas de seguridad definidas para el entorno SCADA, deberá notificar las infracciones/ brechas de seguridad y de la puesta en marcha de las medidas encaminadas a revelar los riesgos que su servicio o proyecto pudiera introducir.

Este interlocutor válido de ciberseguridad, será la referencia principal para la gestión de las diversas tareas de ciberseguridad en los diversos proyectos u operativas suministrada.

3.1.5 Soporte ante incidentes.

La seguridad de la información es un compromiso que afecta a todo el personal de Aena, por lo que deben ser copartícipes de la responsabilidad, garantizando la seguridad de la información en las fases de desarrollo, operación y mantenimiento de los sistemas debiendo notificar cualquier incidente de seguridad.

Así mismo también se debe extender esta responsabilidad a terceros subcontratados.

De esta forma se puede evitar, entre otros ejemplos, que:

- los servicios que presta Aena se vean interrumpidos
- la imagen de Aena se vea afectada
- Aena puede sufrir sanciones económicas
- se pueda incurrir en delitos por incumplimientos normativos
- tus datos personales pueden verse afectados.
-

Las notificaciones se deberán realizar utilizando los canales que se indican a continuación:

- Servicio DTIC H24, a través de:
 - la herramienta Remedy (<http://juno.Aena.es/portal/soporth24/Paginas/inicio.aspx>)
 - A través del correo electrónico dtic.h24@Aena.es
 - telefónicamente en el 91 321 15 11 o en el 211511
- Servicio CSIRT (Centro de Respuesta a Incidentes de Seguridad) de Aena, a través de:
 - Correo electrónico dtic.csirt@anea.es
 - Telefónicamente en el 690 663 590

Cualquier delegación de soporte y responsabilidad de gestión deberá ser aprobada por el Comité de Análisis y Seguimiento de Sistemas SCADA.

3.2 Estudio de seguridad

El estudio de seguridad incluye como punto de partida un estudio de riesgos del sistema que debe ser actualizado y mantenido de forma continua y unas medidas de protección básica cuyo objetivo es incorporar la capa de seguridad al Sistema SCADA.

El estudio de seguridad deberá quedar plasmado en la tabla contenida en el Anexo I de este documento, e incluirá al menos la información solicitada en dicha tabla.

El adjudicatario del desarrollo de un nuevo sistema SCADA o el mantenedor de un Sistema SCADA existente, es el responsable de realizar y mantener actualizado el estudio de seguridad.

3.2.1 Análisis de Riesgos.

El objetivo de realizar un análisis de riesgos es conseguir la mejora de la seguridad de los sistemas de control. Los riesgos del negocio se entienden como una unión de las amenazas, impactos y vulnerabilidades de los sistemas.

Un conocimiento adecuado de los riesgos del negocio permite tomar decisiones informadas sobre los niveles apropiados de protección de los sistemas de la organización.

Además, todas las mejoras de la seguridad deben basarse en el nivel de riesgo a que está sometido un sistema para garantizar el nivel adecuado de protección.

Así mismo es importante determinar la tolerancia del riesgo, esto es, el nivel de riesgo que la organización está dispuesta a asumir.

Para realizar un estudio formal del riesgo es necesario acometer los siguientes puntos:

- Realizar un inventario. Se considera *activo* cualquier componente o funcionalidad de un sistema de información u operación, con valor para la organización y que es susceptible de ser atacado de forma deliberada o accidental con consecuencias para Aena. Los *activos* del alcance deberán ser estudiados ya que son la base para identificar a qué amenazas están expuestos y qué vulnerabilidades contienen, con el fin de determinar la manera en que la materialización de una amenaza afectaría al funcionamiento de los procesos de la instalación. El inventariado de activos deberá estar recogido en el documento Plan de Acción, con el objetivo de que dicho inventariado no se realice de forma individualizada para cada activo, o se incluyan valoraciones subjetivas o personales. Se especifica el proceso de Inventario y gestión de Activos en el apartado 3.2.2.2.1.1 de la presente normativa.
- Estudio de las amenazas. Primero identificar y, posteriormente, evaluar las amenazas a las que se enfrentan los sistemas de control de los aeropuertos. Estas amenazas incluyen denegación del servicio, ataques dirigidos, incidentes accidentales, etc. Las amenazas pueden surgir de una serie de fuentes como son hackers, atacantes internos, personal descontento y otras de distinta naturaleza. Los tipos de amenazas incluyen gusanos, virus, pérdida de disponibilidad, control no autorizado y otros. El estudio de las amenazas por lo tanto debe incluir las fuentes y los tipos.
- Comprender el impacto. Hay que cuantificar el impacto de cada amenaza y su variación con el tiempo.
- Vulnerabilidades. Estudiar las vulnerabilidades implica un examen detallado de todos los elementos del sistema. Estas vulnerabilidades pueden incluir conexiones a otros sistemas, accesos remotos, protección antivirus, parcheados de seguridad, etc.

Se considera que comprender el riesgo del negocio es un proceso continuo, ya que una vez que se ha realizado un estudio del riesgo y se han aplicado las medidas adecuadas y encaminadas de mejora de la seguridad, es importante tener vigilados dichos riesgos y su evolución a medida que pasa el tiempo, puesto que las amenazas pueden cambiar y aparecer nuevas vulnerabilidades. Por lo tanto, el mantenimiento del análisis de riesgos se realizará anualmente, coordinadamente entre el adjudicatario del mantenimiento del sistema y Aena, e incluirá las tareas de revisión y ampliación/adecuación/actualización del inventario, las amenazas, el impacto y las vulnerabilidades de cada Sistema SCADA de su responsabilidad.

3.2.2 Medidas de Protección Básica.

Las medidas de protección básica se establecen con el objetivo de incorporar la capa de seguridad a los Sistemas SCADA de la red de Aeropuertos de Aena, una vez realizado y basándose en el estudio de riesgos e implementada tanto la separación de redes como la segmentación

Debido a las peculiaridades de los aeropuertos desde el punto de vista de que son instalaciones pertenecientes al sector del transporte, pero con un marcado carácter industrial en cuanto a la cantidad y diversidad de instalaciones que los componen, se hace necesario resaltar que el desarrollo e implantación de las soluciones de ciberseguridad aplicadas a los Sistemas SCADA se basan en dos pilares fundamentales.

- **Técnicos-globales:** incluye soluciones dirigidas a implementar la seguridad en los sistemas y aplicativos que componen la instalación, tales como gestión de parches, bastionado, etc.

- Operativos: son los procesos que establecen las políticas y procedimientos que ayudan a fortificar el entorno industrial y la asignación de los procesos a las personas o equipos cuya responsabilidad es identificar amenazas, vulnerabilidades y resolverlas.

En el modelo de desarrollo 1 el encargado de ejecutar estas medidas será el adjudicatario del Sistema (implementación y mantenimiento) y en el modelo 2 será la división correspondiente de la DTIC.

En la siguiente tabla se relacionan las medidas de protección básica de carácter obligatorio. Se recomienda que la implementación se lleve a cabo en la secuencia siguiente:

Controles	Protección básica, carácter obligatorio	Prioridad
Técnico globales	• Gestión de parches • Protección contra malware • Bastionado de sistemas • Protección de acceso • Cifrado • Registro • Distribución de software • Supervisión/monitorización	
Operativos	• Mapa de Procesos • Roles	Después de técnicos

3.2.2.1 Medidas de Control del funcionamiento Técnico del Sistema

3.2.2.1.1 Gestión de Parches.

Para cada componente, se debe comprobar si es posible un proceso periódico de actualización del software del sistema. En caso afirmativo, se debería comprobar previamente para cada actualización si es absolutamente necesaria para el entorno de automatización. Antes de instalar un parche/actualización, éste debe ser probado en el sistema en un entorno de pruebas y autorizado (si está disponible y listo para su implementación).

Debido a los prolongados periodos de funcionamiento, puede darse el caso que haya componentes funcionado más allá de los periodos de vida útil establecidos por el fabricante/OEM.

Esto puede representar que los sistemas operativos o firmware de los componentes individuales no puedan ser objeto de actualización. Estos componentes se convierten en vulnerables frente a las amenazas que surgen a posteriori (p. ej.: rutinas especiales de ataques de programas malignos (malware) o escáneres de vulnerabilidades (analizadores de red/puertos) que no son detectados por los componentes.

Cuando se descarta la posibilidad actualización y se registra esta circunstancia por escrito, deben adoptarse otras medidas de protección. Estas se basan en la segmentación de la red de producción y en la estructura de los puntos de aplicación de políticas de seguridad (PaP) entre cada uno de los segmentos de la red. De este modo podrían minimizarse los daños de un ataque.

Otro riesgo a tener en cuenta es la falta de soporte del hardware (p. ej.: la imposibilidad de sustituir un componente averiado). Una posible estrategia para reducir este riesgo es el almacenamiento apropiado de los componentes de repuesto.

Será de obligado cumplimiento la “Norma de Gestión de Parches de Seguridad” de la DTIC disponible en la siguiente URL:

<https://gdtic.Aena.es/normas/nDTIC/Norma%20de%20Gestión%20de%20Parches%20de%20Seguridad.pdf>

3.2.2.1.2 Protección control Malware.

Se deberán seguir las indicaciones recogidas en el punto 2 de la “Norma DTIC para el uso de las herramientas y medios de microinformática y servidores de RED”, disponible en el enlace:

<https://gdtic.aena.es/normas/nDTIC/Norma%20Microinformática-Servidores%20de%20red.pdf>

Su aplicación será en puestos cliente y servidores.

Además, y en el caso de que mantenedor / instalador, no tenga acceso a las actualizaciones automáticas distribuidas desde la consola ePO, se habilitará un repositorio de red con la última versión de motor y fichero de firmas para su despliegue.

Se deberán tener en cuenta las siguientes medidas e implementarlas en caso necesario

- Debe realizarse un análisis de riesgos que demuestre que existe el nivel de protección apropiado
- Si se da el caso que algunos componentes no pueden ser protegidos contra malware sin restringir o de algún otro modo afectar a la operación, el riesgo tiene que ser minimizado por medio de una zona de seguridad y un software de filtrado de contenidos.
- En el supuesto de un ataque de malware, el tiempo de recuperación de los componentes no protegidos representa un factor determinante a la hora de definir el tamaño de las zonas de seguridad. En estos casos, la zona de seguridad se utiliza para restringir el daño potencial (Caída del sistema, etc.) del área afectada.
- Debe ser requisito la actualización automática de los mecanismos o barreras de protección contra malware (incluyendo las últimas definiciones de malware) cuando las nuevas versiones estén disponibles, de acuerdo con las políticas y procedimientos de Aena.
- Como guía adicional, se deberá considerar el uso de productos software de protección de malware de múltiples fabricantes (ejemplo, utilizando un fabricante en los dispositivos de seguridad de red “NGFW” y otro distinto para los servidores y estaciones de trabajo).
- Prever la gestión de falsos positivos en la detección de malware y su erradicación, para impedir que puedan tener impacto en la disponibilidad de sistema de control. Las actualizaciones han de ser planificadas y adaptadas al plan de continuidad.
- Se deben considerar las recomendaciones de los fabricantes de control de cara a la protección de malware.
- Implantar controles de detección, prevención y recuperación que sirvan como protección contra malware, así como llevar a cabo la implantación de los procedimientos adecuados de concienciación del usuario. Por ejemplo, mediante la instalación y actualización regular de software de detección y limpieza de malware para escanear los ordenadores como control preventivo. La protección contra malware debe estar basada en la detección y reparación del software, concienciación de seguridad y los controles apropiados de acceso a los sistemas y gestión de cambios. Deben considerarse las siguientes guías:
 - Establecer una política formal que prohíba el uso de software no autorizado
 - Establecer una política formal de protección contra los riesgos asociados con la obtención de ficheros y software usando redes externas, o por cualquier otro medio, indicando qué medidas de protección han de tomarse
 - Llevar a cabo revisiones regulares de software y datos contenidos en los sistemas que soportan procesos críticos de operación (la presencia de cualquier fichero no aprobado o autorizado, debe ser investigado formalmente)
 - Instalación y actualización regular de software de detección y reparación para escanear host, medios y flujos de tráfico como medida de precaución o por rutina.
- Para reducir los riesgos del código malicioso, se deberían eliminar cualquier función o servicio superfluo del sistema de control (por ejemplo, VoIP, Mensajería instantánea, FTP, HTTP, email, compartición de ficheros, etc.), realizar un bastionado de los sistemas (Tratado en el siguiente punto).

- Si el software que protege del malware no puede ser desplegado por razones técnicas (por ejemplo, como resultado de falta de soporte del fabricante de la solución o aprobación del mismo, o la imposibilidad de la instalación en tiempos de las actualizaciones), los riesgos resultantes deben ser identificados y otro tipo de contramedidas deben ser implementadas para proveer al menos el mismo grado de protección.

En particular, se deberían tomar en consideración los posibles efectos de los incidentes de malware en equipamiento utilizado para procesos de control en tiempo real y sus comunicaciones asociadas (como sobrecarga o interrupción) y ser mitigados con la implementación de los controles apropiados.

Controles adicionales contra malware

- Securitización de todos los interfaces de datos lógicos y físicos
- Aislamiento de la red e implementación de la segmentación de la red en zonas de seguridad que limiten el impacto de incidentes de malware
- Medidas de robustecimiento (hardening) que minimicen el riesgo de incidentes de malware
- Uso de soluciones basadas en listas blancas, que restringirán la ejecución de cualquier código software

3.2.2.1.3 Bastionado de Sistemas.

Bastionado de sistemas, es la reducción del ámbito de servicios de los componentes sólo a aquellas funciones que son estrictamente imprescindibles. De este modo, se reduce el riesgo de posibles ataques contra funciones o servicios innecesarios o insuficientemente protegidos. Son desactivados o desinstalados los servicios y funciones de los componentes que no son necesarios para producción.

Deben comprobarse cuales son las funciones y servicios de un componente que necesitan indispensablemente ser securizadas y cuáles no. Si el servicio no imprescindible no puede ser desactivado en el propio componente, deberá bloquearse el puerto correspondiente en el punto de aplicación de políticas (PaP) que protege ese componente

El bastionado de equipos deberá seguir las diferentes Normas establecidas por Aena según el equipo a bastionar. El acceso a las distintas normas relativas a este aspecto se encuentra en el siguiente enlace:

<https://gdtic.Aena.es/normas/seguridad/default.aspx>

3.2.2.1.4 Protección de Acceso

3.2.2.1.4.1 Prácticas de gestión de seguridad

Todas las estaciones de trabajo que están conectadas al Sistema SCADA, salvo aquellas que se ubiquen en zonas de acceso restringido, se configurarán para bloquear automáticamente la estación de trabajo o cambiar al entorno de usuario de "solo lectura" después de permanecer inactivo durante 30 minutos o más. La nueva autenticación de la contraseña del último usuario o del administrador del sistema se requerirá para desbloquear la estación.

Todas las estaciones de trabajo, servidores, PLC y equipos de red, como conmutadores o concentradores, se alojarán en armarios o consolas con cierre para evitar el acceso físico al equipo por parte de usuarios no autorizados.

Todos los puertos no utilizados en el equipo de red de control de proceso SCADA se desactivarán.

Todos los eventos de inicio de sesión serán registrados por el sistema. Los eventos de inicio de sesión se registrarán con la fecha y la hora de inicio de sesión, la cuenta de usuario y la ubicación de inicio de sesión. Los registros de inicios de sesión se mantendrán en el sistema por un período mínimo de seis meses.

El sistema debe registrar todos los intentos de inicio de sesión exitosos y fallidos. Si está disponible, se proporcionará funcionalidad para notificar automáticamente al administrador del sistema después de que se hayan excedido cinco intentos de inicio de sesión fallidos consecutivos.

Los intentos fallidos de inicio de sesión no iniciarán un 'bloqueo' automático de la cuenta de usuario.

El sistema debe ser capaz de generar un informe de cuentas de usuario obsoleto. Las cuentas vencidas son cuentas de usuario que no se han usado en el sistema por un período de tres meses o más. El sistema debe producir un informe de cuentas de usuario obsoleto.

3.2.2.1.4.2 Control de Acceso

Para el control de accesos a los Sistemas SCADA, se deberá seguir el procedimiento establecido. Este procedimiento está disponible en la siguiente URL:

<https://gdtic.Aena.es/sitios/dgs/area/windows/grupo/scada/Documentos/Procedimiento%20par%20activaci%C3%B3n%20de%20un%20usuario%20SCADA%20de%20intervenci%C3%B3n.docx>

3.2.2.1.4.3 Roles de usuario

Se definirán los siguientes grupos de acceso, a nivel de Directorio Activo o sistema propietario que permitan las funciones definidas a continuación:

- Administradores: Acceso total a la máquina, permisos de lectura escritura y ejecución sobre sistema operativo y aplicaciones desplegadas. Permisos de instalación
- Operadores: Permisos de acceso y ejecución de aplicaciones. Se permiten cambios en parámetros de la aplicación, para la funcionalidad requerida, nunca a nivel de sistema operativo o Base de datos.
- Consulta: Permite realizar consultas e informes sobre la aplicación.

3.2.2.1.4.4 Cuentas de usuario

Las cuentas de usuario, se generan según el procedimiento establecido en el documento “Norma DTIC para el uso de las herramientas y medios de microinformática y servidores de RED”, punto 5 del documento, disponible en el enlace:

<https://gdtic.Aena.es/normas/default.aspx>

3.2.2.1.4.5 Contraseñas de cuentas de usuario

Se deberán seguir las indicaciones recogidas en el punto 3.7.7 de la “Norma DTIC para el uso de las herramientas y medios de microinformática y servidores de RED”, disponible en el enlace:

<https://gdtic.Aena.es/normas/default.aspx>

Así como los requisitos establecidos en la “Norma de contraseñas”, disponible en el siguiente enlace:

<https://gdtic.aena.es/normas/nDTIC/Norma%20de%20Contraseñas.pdf>

3.2.2.1.4.6 Aplicaciones y cuentas del sistema y contraseñas

Se deberán seguir las indicaciones recogidas en el punto 3.7.2 de la “Norma DTIC para el uso de las herramientas y medios de microinformática y servidores de RED”, disponible en el enlace:

<https://gdtic.Aena.es/normas/default.aspx>

3.2.2.1.5 Cifrado

Hay que aclarar que la utilización del cifrado no debe comprometer la capacidad en tiempo real de los sistemas de producción.

La transferencia de contraseñas no cifradas representa un riesgo para la seguridad de la información. Por este motivo, se deben implementar medidas de reducción de riesgos en el entorno de control. Éstas se describen a continuación.

- La implementación completa de la protección básica es un requisito fundamental para una evaluación posterior.
- No se puede acceder desde el exterior a los sistemas entre los que se transfiere la contraseña.
- Los sistemas tienen que estar securizados.
- El tiempo de inactividad máximo admisible no puede verse comprometido por un reinicio de todos los dispositivos en el área de seguridad en el momento de transferir la contraseña (un reinicio puede ser necesario si se modificó la configuración utilizando una contraseña comprometida).
- Los sistemas no procesan datos confidenciales de ningún tipo.
- La integridad queda asegurada por los procesos posteriores.
- Los accesos físicos (conexiones de red, puertos USB) están protegidos (físicamente o desactivados)

3.2.2.1.6 Distribución de Software

La distribución de software se puede llevar a cabo en modo centralizado utilizando herramientas como WSUS/ SCCM (Windows Server Update Services/ System Center Configuration Manager, anteriormente SMS). WSUS puede ejecutarse sin tener que conectarlo a un dominio de directorio activo. El trabajo administrativo es mayor al que supone una conexión AD. Por regla general, y antes de su distribución el software nuevo se tiene que probar en todos los tipos de dispositivos afectados.

Los dispositivos/software que no soporten una de las soluciones Microsoft antes citadas, deberán comprobarse conjuntamente con el fabricante/OEM para saber si es posible la distribución automática de software (MDT Software).

3.2.2.1.7 Registro

Se deben registrar según lo establecido en el estándar de ciberseguridad IT, los accesos a sistemas críticos, los componentes críticos de la red y la información crítica (crítica = confidencial, secreta, sensible para la integridad o crítica para la continuidad). Los registros tienen que incluir la información necesaria para hacer un seguimiento a las actividades relevantes para la seguridad (implementadas por los administradores, configuración de seguridad modificada) en todos los sistemas afectados. Se deben registrar también todos los accesos al sistema a través de puntos de transferencia (punto de aplicación de políticas (PEP) de seguridad, acceso VPN, Servidor TS Genérico Securitizado) y los cambios de configuración. Todos los registros deben ser clasificados y tratados como confidenciales, críticos para la integridad y disponibilidad - estándar. Para los registros diarios, la evaluación se debe llevar a cabo como mínimo semanalmente.

Cuando se trata de sistema IT no convencionales, se tiene que comprobar primero si el registro es técnicamente posible. Generalmente, el funcionamiento del sistema no debe verse comprometido por el registro.

La monitorización del sistema debe utilizarse para comprobar la eficacia de todos los controles adoptados y para verificar la conformidad con el modelo de política de accesos.

La Oficina de Seguridad TIC de Aena será quien reciba las alertas y avisos de seguridad del sistema de control, así como las acciones pertinentes como respuesta.

Se deben documentar los tipos de acciones a tomar en respuesta a las alertas y avisos, así como mantener contacto periódico con grupos de especial interés (como foros de seguridad).

Se deben generar registros de auditoría de la actividad de usuarios, excepciones y eventos o incidencias de seguridad de la información y mantener dichos registros durante un periodo acordado para servir como prueba en investigaciones futuras y en la supervisión del control de acceso.

3.2.2.1.8 Supervisión/Monitorización

Las actividades de tratamiento de la información, principalmente las actividades relacionadas con la seguridad de la información, deben ser supervisadas de manera continua. Deberán tenerse en cuenta que todas las consolas de supervisión se manejan in situ (esto es, en sistemas/servidores de la localización). Esto garantiza que la supervisión se mantiene operativa en el supuesto de que falle la conexión a Internet/SSCC. Se tienen que supervisar los factores y sistemas siguientes

- Disponibilidad de todos los sistemas de la red de producción
- Informes de errores
- Consolas anti-virus
- IDS/IPS
- Punto de aplicación de políticas de seguridad (acceso, informes, utilización de la capacidad)

Para conseguir un funcionamiento sin errores de los componentes de la red es obligatorio que se supervisen las funciones básicas al objeto de que cualquier problema que surja pueda ser identificado y afrontado en su fase inicial. Además de la supervisión, también es necesaria la incorporación de los sistemas de alarma actuales o nuevos para permitir una reacción rápida a las anomalías identificadas.

Las comunicaciones en los Sistemas de Control Industrial por defecto están en plano o sin seguridad, por lo que como es necesario asegurar dichas comunicaciones tanto en el modelo de desarrollo 1 (responsable el adjudicatario) como en el modelo de desarrollo 2 (responsable Aena), se usará un firewall con módulo IPS con análisis de los protocolos industriales que discurren por la red.

3.2.2.2 Medidas operativas

Las medidas Operativas incluyen los Procesos de Seguridad, y los Roles de Seguridad descritos en los siguientes puntos.

3.2.2.2.1 Procesos de Seguridad

El Mapa de Procesos incluido en la Norma Tecnológica SCADA incluye los siguientes

- Gestión de Activos-. El inventario de activos es el primer elemento de la cadena para aportar seguridad a un sistema. Un inventario de activos incluye un listado de todos los recursos que tienen valor en la organización.
- Gestión de Vulnerabilidades.: Proceso continuo consistente en la identificación, evaluación y corrección de vulnerabilidades en los sistemas y aplicaciones de la organización, entendiendo como vulnerabilidad la debilidad o fallo de los sistemas que ponen en riesgo la seguridad de la instalación, pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad y confidencialidad de la instalación.
- Gestión del Cambio: Ante modificaciones de los componentes en el entorno SCADA, debe crearse un registro exacto de todas las actividades llevadas a cabo de tal forma que se garantice que todas las modificaciones de los componentes en el entorno de SCADA se han llevado a cabo de manera controlada.
- Gestión de Incidentes de seguridad SCADA: Las características del incidente, tipo de recursos afectados y criticidad de los mismos determinará el impacto potencial sobre la instalación, además del orden de prioridad en el tratamiento, en caso de detectarse más de un incidente de forma simultánea.

Los procesos que se indican a continuación se tienen que someter a un proceso de revisión regular por el Comité de Análisis y Seguimiento de Sistemas SCADA.

3.2.2.1.1 Gestión de activos.

La Gestión de Activos se realiza sobre un inventario global que abarca todos los sistemas dentro de su alcance.

La información debe contener los datos del autor, la fecha de autorización, la persona que autoriza, el objetivo y finalidad del proceso, el ámbito de aplicación y otros documentos/anexos aplicables.

Se debe implementar el proceso de gestión de activos de automatización en todas las localizaciones.

El gestor de activos de automatización es el responsable de la introducción y de la mejora continua del proceso de gestión de activos. El Rol Gestor de Activos se define en el punto 3.2.2.2 Roles de Seguridad.

3.2.2.1.1.1 Requisitos mínimos

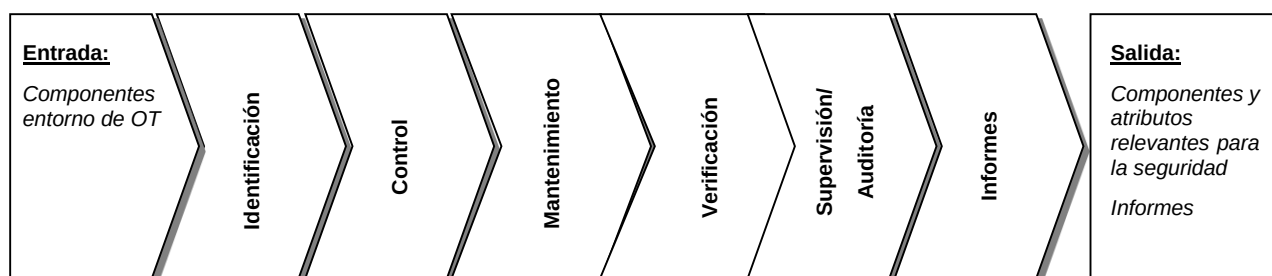
Se tiene que garantizar que la información actualizada esté disponible en todo momento.

- Documentación de los componentes y de sus atributos relevantes para la seguridad. La necesidad de protección de los atributos relevantes para la seguridad debe ser clasificada como mínimo como "confidencial, crítica para la integridad y crítica para la continuidad".
- Deben estar disponibles las copias actuales de los parámetros de configuración de todos los componentes en uso. Mediante la utilización de las tecnologías de control de versiones, debe garantizarse en todo momento la identificación de la última versión.
- Debe llevarse a cabo una evaluación de riesgos de todos los componentes durante todo el ciclo de vida útil (periodo de uso de los componentes en el área de control).

3.2.2.1.1.2 Flujo del proceso

A continuación, se describe los parámetros de entrada del proceso, los pasos y el resultado en modo de cadena genérica del proceso.

Además, se muestran las interfaces principales a otros procesos , funciones, variables, riesgos y documentos de referencia



3.2.2.1.1.3 Pasos del proceso

Los pasos del proceso se describen a continuación de manera genérica y con un alto nivel de abstracción.

- Identificación
 - Identificación de todos los componentes en la red SCADA.

- Asignación de responsabilidad con respecto a los componentes (personal, unidades, etc.).
- Identificación de los componentes en función de su localización, organización y estructura.
- Documentación de los componentes (especialmente los atributos relevantes para la seguridad).
- Definición de KPIs.
- Control
 - Registro de todos los componentes nuevos.
 - Actualización periódica de los componentes y de todos los atributos relevantes para la seguridad asignados.
 - Modificaciones de procedimiento implementadas sólo con peticiones de cambio registradas y aprobadas (garantiza la trazabilidad y documentación).
 - Garantizar la integridad de los datos.
 - Introducción del control de versiones (cuando sea posible, y razonable).
- Mantenimiento
 - Adaptar y actualizar el inventario.
 - Software (software en uso y licencias)
 - Documentación
 - de los respectivos estados (desarrollo, pruebas, activo, vigencia limitada, etc.).
 - del historial
 - El proceso completo de mantenimiento es registrado, autorizado y comunicado.
- Verificación
 - Comprobar a efectos de exactitud e integridad.
 - Llevar a cabo auditorías a intervalos regulares (como verificaciones puntuales/por sorpresa, si fuese necesario).
 - Inmediatamente después de la introducción y documentación de los componentes / atributos.
 - Antes y después de llevar a cabo modificaciones / reajustes en la infraestructura.
 - Después de instalar una nueva versión del software.
 - Después de una recuperación de emergencia.
- Supervisión / auditoría
 - Generación de informes.
 - Llevar a cabo análisis de impacto en el caso que se identifiquen desviaciones.
 - Identificación de modificaciones no aprobadas en el entorno de control.
- Informes

- Informes con arreglo a las variables definidas (KPIs) (tales como número de dispositivos introducidos, número de dispositivos con el estado de actualización actual, diferencia, que dispositivos están en AD, WSUS, etc.).
- Constatación de la necesidad de acción.
- Elaborar informes de las infracciones identificadas.

3.2.2.2.1.2 Gestión de vulnerabilidades de Sistemas SCADA

Proceso que contempla la detección de vulnerabilidades y escenarios de intrusión en Sistemas SCADA a través de un análisis periódico de los componentes del sistema, tal y como se describe a continuación.

La información debe contener los datos del autor, la fecha de autorización, la persona que autoriza, el objetivo y finalidad del proceso, el ámbito de aplicación y otros documentos/anexos aplicables.

Se debe implementar el proceso de gestión de vulnerabilidades en el entorno SCADA.

El Responsable de Seguridad de la Información de Sistemas SCADA es el responsable de la introducción y de la mejora continua del proceso de gestión de vulnerabilidades en el entorno de SCADA. El Rol Responsable de Seguridad de la Información se define en el punto 3.2.2.2 Roles de Seguridad.

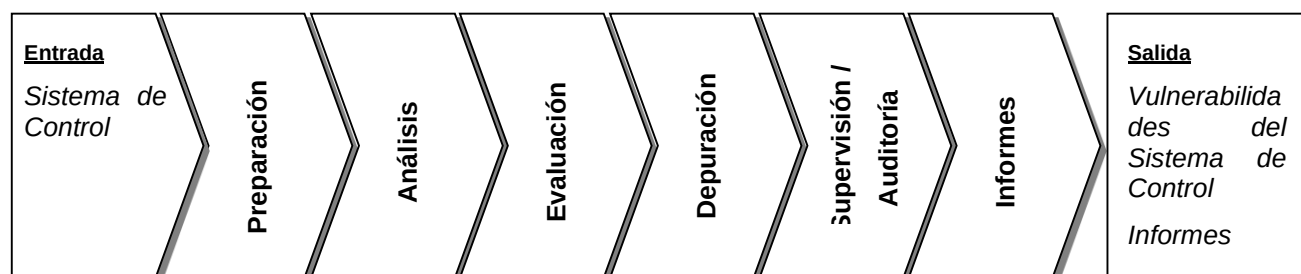
3.2.2.2.1.3 Requisitos mínimos

- Identificación de cuáles son los sistemas que tienen parches o actualizaciones disponibles e instaladas.
- Definición de los requisitos y de los tiempos necesarios para solucionar las vulnerabilidades de seguridad.
- Determinación de un estado predeterminado para que un sistema pueda iniciar de nuevo su funcionamiento en la red SCADA.
- Revisión periódica del proceso global conforme a los requisitos.

3.2.2.2.1.3.1 Flujo del proceso

A continuación, se describe los parámetros de entrada del proceso, los pasos y el resultado en modo de cadena genérica del proceso.

3.2.2.2.1.3.2 Pasos del proceso



Los pasos del proceso se describen a continuación de manera genérica y con un alto nivel de abstracción.

- Preparación
 - Identificación de los Sistemas SCADA

- El inventario está disponible y actualizado.
- Protección de los sistemas de control para asegurar la continuidad del proceso.
- Definición de las métricas de evaluación.
- Definición de indicadores (KPIs)
- Análisis
 - Llevar a cabo un análisis de acuerdo a las métricas de evaluación definidas.
 - Asegurar y evaluar los resultados del análisis.
- Depuración
 - Revisión y depuración de las vulnerabilidades de seguridad.
 - Implementación de medidas de protección adicionales si fueran necesarias.
 - Chequeo de la depuración.
- Supervisión / auditoría
 - Generación de informes.
 - Supervisión y documentación de las vulnerabilidades resueltas y de las que no se pueden resolver.
- Informes
 - Elaboración de informes.
 - Constatación de la necesidad de acción

3.2.2.2.1.4 Gestión del cambio de Sistemas SCADA

El proceso Gestión del Cambio se llevará a cabo siguiendo la Política para la Gestión del Cambio DTIC, según el siguiente documento:

<https://gdtic.Aena.es/normas/pDTIC/Política%20cambios%20tecnologías%20informacion%20y%20comunicaciones.pdf>

El Comité de Gestión de Cambios (CGC) tal y como se define en el documento “Política para la Gestión del Cambio” es el máximo órgano responsable de la aprobación de la ejecución de cambios en los sistemas de información y comunicaciones de los aeropuertos.

3.2.2.2.1.5 Gestión de incidentes de seguridad SCADA

3.2.2.2.1.5.1 Información general del proceso.

La información debe contener los datos del autor, la fecha de autorización, la persona que autoriza, el objetivo y finalidad del proceso, el ámbito de aplicación y otros documentos/anexos aplicables.

Se debe implementar el proceso de gestión de incidentes en el entorno SCADA.

El Coordinador de Seguridad de la Información del Sistema SCADA es el responsable de la introducción y de la mejora continua del proceso de gestión de incidentes en el entorno SCADA. Cualquier incidente de seguridad se comunicará al CSIRT de Aena según lo establecido en el punto 3.1.5. El Rol Responsable de Seguridad de la Información se define en el punto 3.2.2.2.2 Roles de Seguridad.

3.2.2.2.1.6 Requisitos mínimos

- Elaborar informes de incidentes a través de los contactos locales: Elaborar informes de los principales incidentes en la herramienta corporativa, si fuese necesario;
- Definición de: Incidentes de seguridad de la información y problemas de interfaces con sistemas sobrealimentados.

Se deben tener en cuenta las áreas siguientes:

- Acceso autorizado, teniendo en cuenta la identificación del usuario; la fecha y hora de los eventos claves; los tipos de eventos definidos; los archivos/ información a los que se accedió; y los programas que se utilizaron.
- Todas las operaciones que requieren privilegios, tales como
 - La utilización de cuentas de usuarios que requieren privilegios (tales como administrador, operador, mantenimiento, usuario, etc.).
 - Inicio y cierre del sistema.
 - Conexión y desconexión de dispositivos input/output.
 - Intentos de acceso no autorizados como acciones del usuario con error o rechazadas; acciones con error o rechazadas relativas a datos u otros recursos; incumplimiento de las normas de acceso e informe de los puntos de transferencia de red y firewalls; alarmas de los sistemas privados de detección de intrusiones (IDS).
- Errores y alarmas del sistema como
 - Alarmas e informes de la consola;
 - Excepciones a los protocolos del sistema;
 - Alarmas de la gestión de red;
 - Alarmas activadas por sistemas de control de acceso.
- Modificaciones o intentos de modificación de las configuraciones de seguridad en el sistema o de sus medidas de seguridad.
 - Después de su recopilación, los incidentes deben ser analizados minuciosamente;
 - Revisión periódica del proceso global conforme a los requisitos.

3.2.2.2.1.6.1 Flujo del proceso

A continuación, se describe los parámetros de entrada del proceso, los pasos y el resultado en modo de cadena genérica del proceso.



3.2.2.2.1.6.2 Pasos del proceso

Los pasos del proceso se describen a continuación de manera genérica y con un alto nivel de abstracción.

- Identificación y registro de incidentes.
 - Definición de las prioridades y categorías de incidentes
 - Definición de responsabilidades
 - Registro informático de incidentes.
- Clasificación
 - Asignación de prioridades y categorías de incidentes.
 - Asignación del incidente a los grupos/contactos establecidos
- Análisis y Diagnósticos
 - Análisis de incidentes (si fuese necesario, teniendo en cuenta la información de otros procesos).
 - Análisis de incidentes de seguridad de la información con grupos y contactos convenientemente asignados.
 - Información al responsable de seguridad TIC en caso de un incidente de seguridad de la información.
 - Documentación de todas las actividades.
 - Depuración y Registro
 - Desarrollo de una solución para el incidente de seguridad de la información/ fallo.
 - Documentación de la solución.
 - Coordinación de todas las actividades de corrección.
- Supervisión
 - Supervisión de las actividades de corrección.
 - Verificación de la correcta implementación de la solución.
 - Confirmación de la implementación con éxito de la solución.
 - Documentación de todas las actividades.
- Comunicación e Informes
 - Documentación final de todas las actividades de corrección llevadas a cabo.
 - Información al responsable de seguridad TIC de la resolución de un incidente de seguridad de la información.
 - Constatación de la necesidad de acción
 - Determinación de las lecciones aprendidas para futuras actividades en base a los resultados.

3.2.2.2.2 Roles de Seguridad

La creación de Roles de Seguridad establece las bases para organizar el grupo de trabajo responsable de implementar la Norma Tecnológica SCADA, determinando la vinculación de cada actividad descrita en esta norma a un responsable de hacerla, asegurando que todas las actividades o procesos establecidos en el ámbito de seguridad SCADA será realizada por un miembro del equipo.

Cada sistema a implementar o a mantener debe contar con estos roles de seguridad.

3.2.2.2.2.1 Gestor de activos (componentes) de Scada y Control

Descripción	El Gestor de Activos genera y proporciona información acerca de los componentes de automatización y control, SCADA y redes de comunicaciones tanto a nivel hardware como software.
Tareas	• Documentación de los componentes del Sistema SCADA, unidad/accionamiento y red y de los atributos relevantes para la seguridad de redes de operación. • Actualización periódica de la información. • Garantizar que existe un proceso para la documentación de los componentes de Scada y Control, unidad/accionamiento y red y de los atributos relevantes para la seguridad de redes de Scada y Control. • Revisión periódica de la base de datos en cuanto a calidad e integridad.
Responsabilidad	• Adjudicatario del proyecto / Mantenedor del sistema

3.2.2.2.2.2 Responsable de cambios del Sistema SCADA.

El Rol del Responsable de Cambios de SCADA y Control será el designado en el documento “Política para la Gestión de Cambios TIC”, disponible en la siguiente URL:

<https://gdtic.Aena.es/normas/pDTIC/Política%20cambios%20tecnologías%20informacion%20y%20comunicaciones.pdf>

3.2.2.2.2.3 Coordinador de Seguridad de la Información para el Sistema SCADA.

Descripción	Es el responsable de seguridad de la información del sistema y actuará como punto de contacto con el responsable de seguridad de la información de Aena.
Tareas	• Elaborar y proponer los procedimientos para cumplir con la política de seguridad de Aena. Estos procedimientos incluirán las medidas técnicas y organizativas adecuadas para gestionar los riesgos con el fin de prevenir y reducir al mínimo los efectos de los incidentes que afecten a la organización y los servicios.

	• Supervisar la efectividad de las políticas de seguridad, normativas y procedimientos y llevar a cabo las revisiones periódicas de seguridad que se pedirán desde Aena. • Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información tanto en aspectos físicos como lógicos. • Recomendación de medidas para mejorar la seguridad de la información de los entornos SCADA. • Gestión de Riesgos, incluyendo identificación, clasificación y verificación de la arquitectura y diseño del sistema SCADA. • Gestión de Vulnerabilidades para corregir los puntos débiles identificados. • Gestión de Incidentes, que se realizará de acuerdo al procedimiento de Gestión de incidentes de la DTIC y en coordinación con el CSIRT de Aena.
Responsabilidad	• Adjudicatario del proyecto / Mantenedor del sistema

4 Mantenimiento de los sistemas

El objetivo de este punto es establecer de forma clara y concisa el funcionamiento o procedimiento de actuación para el mantenimiento de los diferentes Sistemas SCADAS.

Las responsabilidades y tareas enumeradas a continuación son de obligado cumplimiento tanto en los mantenimientos correspondientes a modelo de desarrollo 1 como a los correspondientes al modelo de desarrollo 2 descritos en el punto 2.1 Diseño de Arquitectura, de este documento.

Las tareas de mantenimiento de instalaciones o Sistemas SCADA que serán de obligado cumplimiento para el responsable de dicho servicio, son las siguientes:

- Para el acceso al Sistema SCADA, se deberá seguir el procedimiento establecido. Este procedimiento en encuentra disponible en la siguiente URL:

<https://gdtic.Aena.es/sitios/dgs/area/windows/grupo/scada/Documentos/Procedimiento%20par%20activaci%C3%B3n%20de%20un%20usuario%20SCADA%20de%20intervenci%C3%B3n.docx>

Ante modificaciones de los componentes en el entorno SCADA, debe crearse un registro exacto de todas las actividades llevadas a cabo de tal forma que se garantice que todas las modificaciones se realizan de manera controlada. Se deberá seguir la Política para la Gestión del Cambio DTIC, disponible en la siguiente URL:

<https://gdtic.Aena.es/normas/pDTIC/Política%20cambios%20tecnologías%20informacion%20y%20comunicaciones.pdf>

- Es obligación del adjudicatario de mantenimiento realizar el análisis de riesgos. Este análisis incluirá las tareas de revisión y ampliación/adecuación/actualización del inventario, las amenazas, el impacto y las vulnerabilidades de cada Sistema SCADA de su responsabilidad. Todo este proceso está definido en el punto “3.2.1 Análisis de Riesgos”.
- Es obligación del adjudicatario de mantenimiento ejecutar las medidas de protección básica en el sistema de su responsabilidad. Estas medidas están establecidas en el punto “3.2.2 Medidas de Protección Básica”.

Se presentan a continuación dos tablas resumen que engloban las tareas necesarias para hacer cumplir la NTS tanto en la etapa de ejecución del proyecto como en la de mantenimiento, la entidad responsable de ejecutarlas y el punto de la norma en el que se explican.

La primera tabla es de aplicación al Modelo de Desarrollo 1 y la segunda al Modelo de Desarrollo 2, esta última tanto para la opción A como para la B.

MODELO DE DESAROLLO 1		
TAREA	RESPONSABLE	REFERENCIA NORMA
Soporte ante incidentes de seguridad	Adjudicatario	3.2.2.2.1.5
Gestión de Activos	Adjudicatario	3.2.2.2.1.1

Gestión de incidentes	Adjudicatario	3.2.2.2.1.5
Gestión de cambios	Adjudicatario	3.2.2.2.1.4
Control de Acceso a la Red	Adjudicatario	2.4.3
Distribución parches de Seguridad	Adjudicatario	3.2.2.1.1
Bastionado de Servidores	Adjudicatario	3.2.2.1.3
Actualización antivirus / Malware	Adjudicatario	3.2.2.1.2
Copias de Seguridad	Adjudicatario	2.4.2
Monitorización	Adjudicatario	3.2.2.1.8
Gestión de usuarios y cuentas privilegiadas de administrador de dominios si existen	Adjudicatario	3.2.2.1.4
Actualización de Software base (S.O. ...)	Adjudicatario	3.2.2.1.6
Desarrollo de aplicaciones SCADA	Adjudicatario	3.2.2.2.2.1
Desarrollo evolutivo de aplicaciones SCADA	Adjudicatario	3.2.2.2.2.2
Actualización software SCADA	Adjudicatario	3.2.2.2.1.2

MODELO DE DESARROLLO 2		
TAREA	RESPONSABLE	REFERENCIA NORMA
Soporte ante incidentes de seguridad	DTIC – OSTIC	3.2.2.2.1.5
Gestión de Activos	DTIC – DGS	3.2.2.2.1.1
Gestión de incidentes	DTIC – OSTIC	3.2.2.2.1.5
Gestión de cambios	DTIC	3.2.2.2.1.4
Control de Acceso a la Red	DTIC - DCOM	2.4.3
Distribución parches de Seguridad	DTIC – DGS	3.2.2.1.1
Bastionado de Servidores	DTIC – DGS	3.2.2.1.3
Actualización antivirus	DTIC – DGS	3.2.2.1.2
Copias de Seguridad	DTIC – DGS	2.4.2
Monitorización	DTIC – DGS	3.2.2.1.8

Gestión de usuarios y cuentas privilegiadas de administrador de dominios si existen	DTIC – DGS	3.2.2.1.4
Actualización de Software base (S.O. ...)	DTIC – DGS	3.2.2.1.6
Desarrollo de aplicaciones SCADA	DTIC - DDAA	3.2.2.2.2.1
Desarrollo evolutivo de aplicaciones SCADA	DTIC – DDAA	3.2.2.2.2.2
Actualización software SCADA	DTIC – DDAA	3.2.2.2.1.2

ANEXO I

ESTUDIO DE SEGURIDAD DEL SISTEMA SCADA		
Descripción Sistema		
Inventario	Si, se adjunta	No se adjunta, se realiza el XX/XX/XXXX
Amenazas	Fuentes	Personal descontento Hackers
	Tipos	Robo de Datos Gusanos Control no autorizado
Impacto		
Vulnerabilidades	Conexiones a otros sistemas Accesos remotos Protección antivirus Parcheos de seguridad	
Medidas de Protección Básicas		
Roles implicados		